Sécurité informatique

Principes et méthode

Laurent Bloch
Christoph Wolfhugel

Préfaces de
Christian Queinnec et Hervé Schauer

Avec la contribution de Solveig,
Florence Henry et Nat Makarévitch

ISBN : 2-212-12021-4
ISBN 13 : 978-2-212-12021-9

EYROLLES

11

Tendances des pratiques de sécurisation des SI

La fin de l'été 2005 a vu la publication de deux articles (*The Six Dumbest Ideas in Computer Security*[1] de Marcus J. Ranum et *The Next 50 Years of Computer Security : An Interview with Alan Cox* par Edd Dumbill[2]) qui sont appelés à faire date dans le domaine de la sécurité informatique : en effet ils réservent un sort cruel à quelques idées reçues et à quelques intuitions largement partagées. Le présent chapitre, à la faveur d'une étude de ces articles, aborde plusieurs questions fondamentales : les systèmes de détection ou de prévention d'intrusion, ainsi que la protection de la propriété *et* de la liberté intellectuelles dans un monde numérique.

[1] Cf. `http://www.ranum.com/security/computer_security/editorials/dumb/`
[2] Cf. `http://www.oreillynet.com/pub/a/network/2005/09/12/alan-cox.html`

Les six idées les plus stupides en sécurité, selon Ranum

Marcus J. Ranum m'a autorisé à faire ici de larges emprunts à son article, qu'il en soit remercié. S'il fallait résumer en une idée générale les thèses qu'il défend et qu'il illustre, ce serait que, si l'on veut construire un système informatique (au sens large) sûr, il faut que la sécurité soit incorporée à sa conception dès l'origine : il est coûteux et inefficace de vouloir « ajouter de la sécurité » *a posteriori* à un système conçu sans idée de sécurité au départ. Le corollaire de cette idée, c'est qu'il est possible de concevoir un tel système, que les méthodes existent pour ce faire, et M.J. Ranum en donne quelques exemples. Nous avons d'ailleurs eu l'occasion à la page 89 de décrire un système conçu selon ces principes dès 1964, Multics.

Marcus J. Ranum est un pionnier de la sécurité des systèmes d'information ; inventeur de la notion de pare-feu *(firewall)*, il en a également signé la première réalisation à la fin des années 1980 ; il a aussi joué un rôle précurseur dans le développement des systèmes de détection d'intrusion. Nous allons présenter et discuter ses six propositions[3]. Mais nous pouvons, avant de commencer, être déjà d'accord avec lui pour dire que si votre politique de sécurité est indigente et si les règles que vous fixez sont insuffisantes ou incohérentes, aucun pare-feu de grand luxe ne protégera votre site, eût-il coûté 100 000 euros.

Idée stupide n° 1 : par défaut, tout est autorisé

Cette idée ne demande pas un long examen pour être classée en première place dans la liste des stupidités. Il est assez clair que les conditions actuelles sur les réseaux exigent que par défaut tout soit interdit, et que ne soient autorisées que les actions effectivement et positivement identifiées comme légitimes. Mais cette idée stupide, si facile à réfuter en apparence, est incroyablement résiliente et envahissante.

C'est bien sûr dans la rédaction des règles de pare-feu que cette idée stupide numéro 1 se manifeste en priorité : on laisse passer par défaut tous les types de trafic et on bloque ceux que l'on estime dangereux ; une variante consiste à bloquer pas mal de choses mais à aligner une longue liste de dérogations qui, outre le fait qu'elles vont détériorer les performances de l'accès au réseau, vont anéantir la sécurité, parce que ces dérogations seront autant de portes assez faciles à ouvrir, par exemple par usurpation d'adresse IP, l'enfance de l'art pour un pirate amateur.

[3] `http://www.ranum.com/security/computer_security/editorials/dumb/`

Nous serons d'accord avec M. Ranum pour dire que la véritable bonne idée, c'est « par défaut, tout est interdit ».

Idée stupide n° 2 : prétendre dresser la liste des menaces

Cette idée stupide numéro 2, en fait assez voisine de sa sœur la numéro 1, pourrait aussi s'incarner dans une configuration de pare-feu établie en fonction de la liste des menaces recensées. Elle est stupide car en 2006 la liste des menaces est très longue, et surtout elle s'accroît chaque jour : les recenser pour mettre son pare-feu à jour s'apparente au remplissage du tonneau des Danaïdes. Les listes auxquelles je suis abonné publient une dizaine de nouvelles *vulnérabilités* par semaine, et on estime entre 200 et 700 par mois le nombre de nouvelles *menaces*.

Le délai qui s'écoule entre la découverte d'une vulnérabilité et son exploitation par un logiciel menaçant est passé en quelques années de quelques mois à une quinzaine de jours dans certains cas. C'est-à-dire que le logiciel nuisible peut apparaître avant la correction de la vulnérabilité, et que même si ce n'est pas le cas il peut suffire d'un retard de quelques heures dans l'application de la correction pour être exposé sans défense à la menace. Et n'oublions pas que les pirates, présents dans tous les fuseaux horaires, agissent durant nos nuits et nos jours fériés. Bref, en 2006 il est effectivement stupide d'espérer assurer la sécurité de son SI en se prémunissant contre des menaces qui seraient connues d'avance.

Il faut au contraire dresser la liste de tous les logiciels *utiles*, d'usage légitime dans le SI de l'entreprise, et interdire tous les autres en vertu de la règle précédente.

Ainsi, considérons un projet de sécurité informatique destiné à évaluer et à améliorer la disponibilité d'un système d'information. Si le responsable du projet s'inspire de la méthode EBIOS élaborée en France par la Direction centrale de la sécurité des systèmes d'information (DCSSI), il dressera une liste des risques, associera chacun de ces risques à des vulnérabilités, et envisagera les contre-mesures qu'il peut élaborer pour s'en prémunir, selon une formule pleine de bon sens et d'utilité[4] :

$$\text{risque} = \frac{\text{menace} \times \text{vulnérabilité} \times \text{sensibilité}}{\text{contre-mesure}}$$

[4]Nous avons donné à la page 7 une autre formule pour le risque, qui complète utilement celle qui va suivre.

Cette conceptualisation paraît intéressante, la formule multiplicative permet de classer les risques selon un ordre de priorité en fonction de leur intensité concrète pour l'entreprise, par opposition à une intensité technique perçue par l'ingénieur de sécurité, mais elle peut engendrer la tentation de dresser une liste de risques ou une liste de vulnérabilités que l'on placera dans la colonne de gauche d'un tableau, afin d'en remplir la colonne de droite avec les contre-mesures appropriées.

Pourquoi cette démarche est-elle maladroite ? Parce que les risques et les menaces sont nombreux et souvent inconnus, alors que le répertoire des contre-mesures possibles est beaucoup plus réduit ; souvent, cela peut se résumer à cinq ou six grands thèmes : plan de sauvegarde des données, amélioration du stockage, aménagement d'un site de secours avec duplication des données à distance, administration correcte des serveurs (fermeture des services inutiles, séparation des privilèges, application des correctifs de sécurité, surveillance des journaux), sécurisation du réseau (pare-feu, authentification forte, fermeture des services inutiles), sécurisation physique des locaux. Il est donc plus simple et plus efficace de partir de la table inverse de la précédente : mettre les contre-mesures dans la colonne de gauche, et énumérer dans la colonne de droite les risques éliminés par elles, ce qui évitera de payer un consultant pendant des mois pour élaborer la liste des centaines de risques plus ou moins réels que l'on peut envisager.

Idée stupide n° 3 : tester par intrusion, puis corriger

La mise en pratique de cette idée stupide numéro 3 consiste à détecter les failles du système à protéger en perpétrant une intrusion, en d'autres termes, à attaquer son système de protection, pare-feu, antivirus ou autre, puis à obturer les brèches que l'on aura détectées. Cette idée stupide est mise en œuvre par de nombreux cabinets spécialisés, qui proposent des *tests d'intrusion* à leurs clients, lesquels, lorsqu'ils sont incompétents, sont friands de ce genre d'exercice.

M. Ranum observe que, si la sécurité par test d'intrusion et correction était une bonne méthode, les failles d'*Internet Explorer* seraient corrigées depuis longtemps. Il observe également que certains logiciels, comme *Postfix* ou *Qmail*, sont quasiment exempts de failles depuis leur naissance, et ce parce qu'ils ont été conçus dès l'origine pour ne pas en comporter, c'est-à-dire que leur réalisation s'est appuyée sur des méthodes à l'épreuve des failles.

M. Ranum en vient là à son idée centrale : la seule façon d'obtenir un système sûr, c'est qu'il le soit dès la conception, et c'est possible. Nous pourrions qualifier ce principe de *méthode de sécurité a priori*, par opposition aux méthodes de sécurité *a posteriori*, qui consistent à construire des systèmes non sûrs, puis à essayer de les réparer en détectant les failles *a posteriori*. Par analogie, nous pourrions dire que la méthode en usage dans la Marine Nationale et connue par la devise « Peinture sur rouille[5] égale propreté » ne donne pas en matière de sécurité des résultats satisfaisants.

M. Ranum conclut sur ce point en indiquant que si votre système est régulièrement vulnérable au « bug de la semaine », c'est que vous êtes dans la configuration évoquée ici, et que tout pirate qui inventera une attaque nouvelle réussira chez vous.

Idée stupide nº 4 : les pirates sont sympas

« La meilleure façon de se débarrasser des cafards dans la cuisine, c'est de jeter les miettes de pain sous la cuisinière, c'est bien connu », nous dit ironiquement M. Ranum, avant de citer Donn Parker :

« L'informatique en réseau a affranchi les criminels de la contrainte historique de proximité avec leur crime. L'anonymat et l'exemption de la confrontation personnelle avec la victime ont diminué la difficulté émotionnelle à commettre un crime, parce que la victime n'est qu'un ordinateur inanimé, pas une personne ou une entreprise réelles. Les gens timides peuvent se mettre au crime. La prolifération de systèmes identiques, de moyens d'y accéder et l'automatisation des transactions commerciales permettent et favorisent l'économie du crime automatisé, la réalisation d'outils criminels de grande puissance et l'apparition de scénarios très rentables. »

La criminalité informatique est un problème social, pas une question de technologie, nous dit M.J. Ranum. La diffusion de l'informatique a donné un champ d'action élargi à certaines personnes dépourvues de maturité et mal socialisées, auxquelles les médias accordent une publicité assez déplacée en les présentant comme de brillants informaticiens dont les grandes entreprises en mal de sécurité se disputeraient les services à coup de super-salaires et de stock-options. Le

[5] Cette locution proverbiale m'était venue sous une forme légèrement différente, mais Christian Queinnec m'a permis de la rectifier.

fait que les pirates soient de plus en plus souvent des criminels organisés qui détournent des sommes importantes finira par avoir raison de cette idée idiote. La majorité des autres pirates sont des adolescents attardés et incompétents, qui se contentent de propager des logiciels malfaisants tout faits qu'ils n'ont eu que la peine de télécharger sur le Net.

Corollaire tout aussi idiot de cette idiotie n° 4, l'idée que les responsables de sécurité du SI devraient s'initier aux techniques de piratage : outre qu'un tel apprentissage serait pratiquement à recommencer chaque semaine, il absorberait en pure perte une énergie qui, pendant ce temps, ne serait pas consacrée à l'édification de systèmes et de réseaux sûrs *par construction*.

Idée stupide n° 5 : compter sur l'éducation des utilisateurs

Ceci semble un paradoxe : on ne reçoit jamais trop d'éducation ! Il s'agit ici de l'application de l'idée stupide n° 3 aux êtres humains : attendre que les utilisateurs aient été victimes d'un incident de sécurité et d'attaques réussies, et ensuite seulement les corriger (éduquer). En fait tout semble indiquer qu'une proportion importante d'utilisateurs seront toujours prêts, quoi qu'il advienne, à cliquer sur un lien qui promet une image pornographique ou de l'argent facile ; la nature humaine est ainsi faite, on ne la corrigera pas. Il faut donc arriver à la conclusion suivante :

Si votre politique de sécurité repose sur l'éducation des utilisateurs, alors elle est vouée à l'échec.

D'ailleurs, l'idée que l'on puisse corriger chez l'homme la propension à commettre les actes évoqués ici est une idée encore plus détestable que l'insécurité des systèmes d'information. Mieux vaut donc configurer le système de sorte que :

1. les choses dangereuses ne parviennent pas aux utilisateurs ;
2. lorsque certaines choses dangereuses passent à travers les mailles du filet (il y en aura), les conséquences en seront limitées, détectées puis contrôlées.

Cela étant dit, il faut, bien sûr et dans la mesure du possible, faire l'éducation des utilisateurs.

Idée stupide nº 6 : l'action vaut mieux que l'inaction

M. Ranum vise ici, plutôt que l'action, l'activisme. Il est clair que le responsable de site qui veut toujours adopter avant tout le monde les plus récentes technologies s'expose davantage à des incidents de sécurité que l'administrateur prudent qui attend deux ans la stabilisation du système et les retours d'expérience avant de l'implanter. En outre, pendant ce délai le coût induit par le déploiement aura probablement diminué.

On peut aussi citer l'aphorisme suivant : « Il est souvent plus facile de ne pas faire quelque chose d'idiot que de faire quelque chose d'intelligent » (attribué abusivement à l'*Art de la guerre* de Sun Tzu).

Quelques idioties de seconde classe

M. Ranum énumère pour finir quelques assertions et pratiques stupides de moindre ampleur :

- « Nous ne sommes pas une cible intéressante » : or, tout le monde est visé, les vers et les virus ne sont pas capables d'identifier les cibles qui en valent la peine ;
- « en déployant < *mettre ici le nom de votre système ou pare-feu préféré* > nous serons protégés » : non, le système ou le pare-feu qui protège, c'est celui pour lequel il y a sur le site un ingénieur (oui, un ingénieur, les gens qui savent faire ça sont des ingénieurs) compétent, qui le connaît bien et qui consacre beaucoup de son temps à s'en occuper ;
- « pas besoin de pare-feu, notre système est sûr » : non, même avec un système sûr, sans pare-feu toute application réseau est une cible facile ;
- « pas besoin de sécuriser le système, nous avons un bon pare-feu » : non, le trafic légitime qui franchit le pare-feu comporte des risques ;
- « démarrons la production tout de suite, nous sécuriserons plus tard » : non, ce ne sera jamais fait, et si cela doit l'être, cela prendra beaucoup plus de temps et de travail que de l'avoir fait au départ ;
- « nous ne pouvons pas prévoir les problèmes occasionnels » : si, vous pouvez ; prendriez-vous l'avion si les compagnies aériennes raisonnaient ainsi ?

Les cinquante prochaines années, selon Alan Cox

Alan Cox est un des principaux développeurs du noyau Linux, qu'il a notamment contribué à doter de la capacité de préemption. Il est intéressant de relever ce qu'il considère comme des facteurs de progrès de la sécurité des systèmes informatiques, en partant de son jugement sur la situation actuelle d'insécurité, qu'il estime insoutenable :

1. l'essor des systèmes de vérification de code (cf. page 98), et surtout de leur utilisation ;
2. l'amélioration des méthodes de développement, avec des langages comme Java qui règlent la majeure partie des problèmes d'allocation mémoire, principale source de failles comme l'on sait (voir page 92) ;
3. une gestion plus fine et plus restrictive de l'attribution des privilèges aux utilisateurs ;
4. les techniques de *défense en profondeur* (cf. page 13) se répandent : ainsi, le choix d'adresses aléatoires (ou plutôt imprévisibles) pour l'implantation des objets en mémoire, le verrouillage par le matériel ou par le logiciel de certaines régions de mémoire rendues non exécutables, l'usage de systèmes sécurisés comme *SELinux* (une version blindée de Linux), etc.

Détection d'intrusion, inspection en profondeur

C'est ici encore à Marcus J. Ranum[6] que nous ferons appel pour discuter la question de l'*inspection en profondeur* ; dans l'article que nous évoquons ici et dont nous retraçons les grandes lignes, il entreprend de démontrer la supériorité du mandataire applicatif sur les différents systèmes de détection et de prévention des attaques. Cet article se situe dans la droite ligne de celui que nous avons présenté au début de ce chapitre[7], en cela il défend les principes des *méthodes de sécurité a priori*, ou par construction, par opposition aux méthodes de sécurité *a posteriori*, ou curatives.

[6] `http://www.ranum.com/security/computer_security/editorials/deepinspect/`
[7] `http://www.ranum.com/security/computer_security/editorials/dumb/`

Pare-feu à états

Nous avons vu, à la section consacrée aux pare-feu (page 125), que les techniques traditionnelles de filtrage n'étaient plus suffisamment efficaces pour bloquer les attaques modernes perfectionnées, et que les pare-feu modernes utilisaient de plus en plus les techniques de suivi de connexion, qui consistent à garder en mémoire une séquence de paquets de façon à en faire l'analyse longitudinale, ce qui permet de détecter certaines malfaisances subtiles, notamment par la défragmentation de datagrammes IP et le ré-assemblage de segments TCP. Les pare-feu qui utilisent cette méthode, inaugurée en 1993 par la firme *Checkpoint*, sont appelés *stateful firewalls*, ou pare-feu à états.

Détection et prévention d'intrusion

La vague suivante de produits de sécurité fut celle des systèmes de détection et de prévention d'intrusion, dont le modèle libre est le logiciel *Snort*. Ces logiciels utilisent une base de données de signatures de vers et d'autres logiciels malfaisants, un peu à la manière d'un antivirus, et se sont révélés relativement efficaces contre la grande épidémie de vers des années 2001 à 2004, mais leur vogue décline au fur et à mesure que leur efficacité diminue. La base de signatures de *Snort* contient les descriptions de plus de 3 000 attaques.

Inspection en profondeur

Une autre voie, illustrée par certains fournisseurs (Checkpoint, Netscreen), est le pare-feu à inspection en profondeur de paquets. Il s'agit en fait d'un pare-feu à états auquel on aurait greffé la base de signatures d'un système de prévention d'intrusions, et en outre quelques procédures de détection d'anomalies protocolaires.

Critique des méthodes de détection

Dans son article cité en référence, Marcus J. Ranum cite en exemple de procédure d'inspection en profondeur l'analyse du protocole SMTP par le logiciel NFR : ce logiciel examine la séquence complète de commandes SMTP du début à la fin de l'envoi de message, et émet une alerte en cas d'occurrence d'une commande `Mail From :` émise par le logiciel client avant la commande `RCPT To :` correspondante ; une telle analyse est très efficace, parce qu'un logiciel de messagerie de

bonne foi n'utilisera *jamais* une telle séquence, et qu'il ne peut s'agir que d'une anomalie, d'une tentative de piraterie. Mais, dans cet exercice, un pare-feu à base de mandataire applicatif sera supérieur à un système de détection d'anomalies protocolaires, parce que par définition le mandataire *exécute* le protocole, et que de ce fait aucune anomalie ne peut lui échapper. Alors que le système de détection en est réduit à *supputer* ce que le protocole exécute, le mandataire *est* l'implantation du protocole.

Comme un mandataire applicatif exécute les séquences protocolaires pour lesquelles il a été programmé dès sa conception, il n'accomplit, par construction, que des actions autorisées, il réalise le principe « par défaut, tout est interdit ».

Le logiciel de détection d'attaques examine sa base de données de signatures d'attaques, et s'il ne trouve aucune signature qui corresponde à la séquence examinée, il considère qu'elle est légitime, ce qui réalise le principe « par défaut, tout est permis ».

Face à des profils d'attaques de plus en plus nombreux, de plus en plus divers et de plus en plus complexes, nous pensons que dans la course aux armements entre attaquants et systèmes de détection, les attaquants submergeront tôt ou tard les défenseurs, et nous nous rangerons à l'avis de Marcus J. Ranum : l'avenir est au mandataire applicatif.

À qui obéit votre ordinateur ?

En ce début de siècle obsédé par des menaces contre la sécurité et l'ordre public se manifestent des tendances au renforcement du contrôle social, qui, dans le domaine qui nous intéresse ici, se traduisent par de vastes projets de surveillance des usages des ordinateurs et des réseaux, et d'interdiction de ceux de ces usages qui ne reçoivent pas l'assentiment des puissances à l'œuvre dans l'industrie des médias, par exemple pour ce qui touche à la diffusion et à l'échange de musique et de films par l'Internet. Ces tendances répressives constituent un danger parce que, comme toutes les mesures excessives et abusives, elles se retournent contre leur objectif initial : elles se révèlent nuisibles à la disponibilité et à la liberté d'usage légitime des systèmes d'information, tout en concentrant un pouvoir excessif dans les mains d'un petit nombre d'entreprises privées.

Conflit de civilisation pour les échanges de données numériques

L'ubiquité de l'informatique et de l'Internet jusque dans les habitudes domestiques et culturelles a engendré de nouveaux comportements dans la vie privée des citoyens, au nombre desquels la publication de sites Web privés tels que les blogs, l'échange de conversations et de documents de toute sorte par le réseau, qu'il s'agisse de textes, d'images ou de sons, ainsi que de nouvelles formes de créativité, puisque tel qui était mauvais dessinateur au fusain et au canson peut se révéler brillant graphiste électronique, et tel autre qui souffrait du symptôme de la page blanche avec un stylo frise la graphomanie avec un clavier et un écran. Ces nouvelles pratiques culturelles sont souvent associées à l'usage de logiciels libres, ou fécondées par eux. Elles ont considérablement élargi le champ de la liberté d'expression, et apparaissent comme une évolution majeure de la civilisation et de la culture.

Cette véritable révolution culturelle rencontre l'hostilité des industriels de la culture ; rappelons ici quelles sont les grandes puissances de cette industrie : le marché mondial de l'édition numérique (CD et DVD) est contrôlé par quatre géants, les « majors », EMI, Sony, TimeWarner et Universal. Ces industriels de la culture, au lieu de s'adapter à ces évolutions en imaginant de nouvelles formes de commerce, comme Amazon a bien su le faire, ont préféré s'engager dans un combat conservateur (perdu d'avance) pour préserver leurs rentes, assises sur des technologies vieillissantes vendues à des tarifs surévalués, et faire interdire les nouvelles pratiques culturelles évoquées ci-dessus. À cette fin ils se sont engagés dans un combat juridico-technique planétaire pour faire adopter par les États des législations prohibitionnistes à l'encontre des nouvelles pratiques de création et d'échange, qui reposent sur les ordinateurs et le réseau.

Le combat juridique se double d'un combat technique. En fait, l'offensive des majors avance sur deux fronts :

- créer des dispositifs techniques destinés à empêcher ou à surveiller les pratiques jugées indésirables par les majors ; nous avons eu l'occasion de décrire un de ces procédés à la page 58 ; dans cette entreprise ils reçoivent le soutien de certains industriels de l'informatique, notamment Intel et Microsoft ;
- faire adopter par les États des législations qui interdisent le contournement de ces dispositifs techniques, et qui permettraient de punir les pratiques désapprouvées par les majors.

Cette combinaison de dispositions techniques et légales devrait être verrouillée, si les rêves des majors se réalisent, par l'adoption en Europe d'une législation sur la brevetabilité du logiciel, inspirée de celle qui a cours aux États-Unis, et qui pourrait empêcher la création de logiciels libres, notamment dans ce domaine de la création et de la diffusion d'œuvres de l'esprit. Dans ce combat des brevets logiciels, les majors ont reçu le renfort de Siemens, Nokia, Philips et Alcatel. Autant dire que les forces hostiles aux nouvelles pratiques culturelles disposent de moyens économiques et de pouvoirs d'influence considérables.

Dispositifs techniques de prohibition des échanges

Gestion des droits numériques (DRM)

Nous avons déjà évoqué à la page 58 le protocole de gestion des droits numériques DRM, en l'occurrence pour en signaler une réalisation fautive et frauduleuse. DRM vise à protéger des données numériques enregistrées sur CD ou DVD, ou diffusées par le réseau, au moyen d'un système de chiffrement et de signature. Le fichier numérique qui contient, par exemple, le film ou la musique est chiffré et compressé. Il ne pourra être lu qu'au moyen d'un logiciel spécial, qui sera éventuellement fourni avec le fichier et installé sur le même support. Pour lire le fichier, c'est-à-dire voir le film ou écouter la musique, l'acheteur devra fournir une clé secrète qui lui aura été remise au moment du paiement. Le logiciel DRM pourra également, au gré du vendeur, limiter le nombre de copies possibles du fichier, ou le nombre de lectures, ou la date limite de lecture.

Un des multiples inconvénients du protocole DRM, c'est qu'il limite l'usage légitime des données qu'il protège : si le logiciel de lecture ne fonctionne que sur tel ou tel modèle de lecteur de DVD ou avec tel ou tel système d'exploitation, les propriétaires de systèmes différents ne pourront pas utiliser le DVD en question, quand bien même ils l'auront payé, et la loi sur les brevets logiciel leur interdira de créer un logiciel libre destiné à résoudre ce problème. La situation décrite ici n'est pas du tout un cas d'école, elle s'est effectivement produite ; ainsi le Norvégien Jon Johansen a été poursuivi en 2000 par les tribunaux de son pays, à la demande de l'Association américaine pour le contrôle de la copie de DVD (DVD-CAA), pour le simple fait d'avoir tenté de lire ses propres DVD, et d'avoir écrit pour ce faire le logiciel DeCSS pour le décodage des DVD sous Linux ; il a finalement été

acquitté en 2003. Et on ne compte plus les acheteurs dépités de ne pas pouvoir lire leur DVD tout neuf sur leur lecteur tout neuf, grâce à DRM.

Trusted Computing Platform Alliance (TCPA)

Trusted Computing Platform Alliance est une association d'entreprises d'informatique (HP, IBM, Intel, Microsoft...) qui se donne pour objectif la sécurité des équipements et des réseaux informatiques, et qui développe pour cela des dispositifs matériels et logiciels qu'elle souhaite incorporer au cœur des ordinateurs et des systèmes d'exploitation de demain. Ce qui est à noter, c'est que les dispositifs envisagés par TCPA sont destinés à être implantés dans des couches basses du matériel et du logiciel, de telle sorte que l'utilisateur ne pourra pas intervenir pour modifier leur comportement.

Le principe des dispositifs TCPA consiste à attribuer une signature à chaque élément de système informatique (logiciel, document), et à déléguer à un tiers de confiance la possibilité de vérifier si l'objet considéré peut être légitimement utilisé sur le système informatique local.

Tout élément non signé ou dont la signature n'est pas agréée par le tiers de confiance sera rejeté. On imagine les applications d'un tel dispositif à la lutte contre les virus. Mais aussi, si par exemple le « tiers de confiance » est le fournisseur du système (et qui pourra l'empêcher de s'arroger cette prérogative ?), il lui sera possible de vérifier que les applications utilisées sont bien conformes au contrat de licence concédé à l'utilisateur. Un des problèmes soulevés par cette technique est que l'utilisateur final perd ainsi toute maîtrise de ce qui peut ou ne peut pas être fait avec son propre ordinateur. C'est par ce procédé, notamment, qu'Apple s'assure que son système d'exploitation Mac OS X ne peut être exécuté que sur les ordinateurs à processeur Intel de sa fabrication. Mais on pourrait imaginer que cette méthode soit utilisée pour empêcher l'usage de certains logiciels libres.

Les spécifications émises par TCPA formulent la définition du *Trusted Platform Module* (TPM), destiné à procurer des *primitives de sécurité* dans un environnement sûr. Par « primitives » on entend : signature électronique, génération de nombres pseudo-aléatoires, protection de la mémoire, accès à un état garanti de l'information contenue par le TPM. L'intégrité et l'authenticité de ces primitives et de leur exécution sont assurées par des dispositifs matériels. Le TPM doit être

un composant discret, identifiable de façon distincte sur la carte-mère de l'ordinateur, mis en œuvre au moyen d'un pilote activé par le BIOS. Ces dispositions assurent l'indépendance du fonctionnement du TPM à l'égard de ce qui se passe dans le système accessible à l'utilisateur. Par exemple, l'utilisation du TPM peut garantir qu'un dispositif de DRM n'aura pas été modifié ou contourné par un utilisateur, opération triviale avec les dispositifs de DRM actuels, implantés purement en logiciel.

Next-generation secure computing base (NGSCB)

Next-generation secure computing base est le nom d'un projet Microsoft antérieurement baptisé Palladium. NGSCB devait être utilisé par Microsoft pour implanter une architecture de confiance dans son système le plus récent, *Vista*, mais cette installation est différée *sine die*, sans doute à cause des réticences suscitées par les aspects *Big Brother* prêtés au système.

Avec NGSCB, qui fonctionne à l'aide d'un processeur cryptographique, le système d'exploitation *Vista* travaillera dans un environnement de sécurité. Les principes en sont d'incorporer la cryptographie au système d'exploitation pour garantir l'intégrité des échanges entre processus, entre les processus et la mémoire, entre les processus et les disques, et entre les processus et les dispositifs d'entrée-sortie (clavier, souris, écran...).

Ce mode de fonctionnement permettrait de vérifier que des fichiers créés par une application ne peuvent être lus ou modifiés que par cette même application ou par une autre application autorisée, de protéger le système contre l'exécution de codes non autorisés tels que les virus et tout programme non autorisé par l'utilisateur ou l'administrateur, et de mener à bien l'édification de systèmes informatiques vraiment distribués dont chaque composant puisse faire confiance aux autres parties du système (logicielles ou matérielles) même si celles-ci font partie d'un système distant.

Les détracteurs du projet ne manquent pas d'observer qu'avec NGSCB Microsoft aura les moyens d'exercer un contrôle total sur les ordinateurs de ses clients, et notamment d'y persécuter les logiciels libres qu'il estimerait contraires à ses intérêts. Un tel dispositif sera aussi de nature à accroître l'efficacité des systèmes de DRM... et à aggraver les abus qui en découlent, signalés ci-dessus.

Les développements récents de cette politique de contrôle des usages sont évoqués par la revue *Microprocessor Report* [70] : les industriels prévoient de lancer une offre de diffusion vidéo haute définition à la demande par l'Internet, qui sera encadrée par des mesures techniques de protection drastique, en l'occurrence les plates-formes matérielles *Viiv* d'Intel ou *Live !* d'AMD, le procédé de chiffrement HDCP *(High Bandwidth Digital Content Protection)* et le dispositif de connexion HDMI *(High Definition Multimedia Interface)*. Tout cela signifie qu'il faudra, pour accéder à cette offre, faire l'emplette d'un nouvel ordinateur et d'un nouveau système d'exploitation, et que les systèmes libres tels que Linux ou OpenBSD en seront probablement exclus.

Informatique de confiance, ou informatique déloyale ?

Richard M. Stallman a écrit un article[8] de critique de ces projets qui prétendent nous mener vers une informatique « de confiance », où il la qualifie, au contraire, d'*informatique déloyale*. La déloyauté réside dans les possibilités que NGSCB offre au « tiers de confiance » pour agir sur les données stockées par l'ordinateur, à l'insu de l'utilisateur légitime et sans que celui-ci puisse rien faire pour l'empêcher. R.M. Stallman donne des exemples d'actions déloyales rendues possibles par de telles techniques :

« Rendre impossible le partage des fichiers vidéos et musicaux est une mauvaise chose, mais cela pourrait être pire. Il existe des projets pour généraliser ce dispositif aux messages électroniques et aux documents – ayant pour résultat un e-mail qui disparaîtrait au bout de deux semaines, ou des documents qui pourront seulement être lus sur les ordinateurs d'une société mais pas sur ceux d'une autre. (...)

Les logiciels de traitement de texte tels que Word de Microsoft pourraient employer « l'informatique déloyale » quand ils enregistrent vos documents, pour s'assurer qu'aucun autre traitement de texte concurrent ne puisse les lire. (...)

Les programmes qui utilisent « l'informatique déloyale » téléchargeront régulièrement de nouvelles règles par Internet, et imposeront ces règles automatiquement à votre travail. »

[8] `http://www.gnu.org/philosophy/can-you-trust.fr.html`

Nous trouvons sur le site de l'Adullact[9] une analyse comparative des licences logicielles, qui corrobore les craintes que l'on peut avoir à l'égard des mesures techniques de protection associées à la gestion des droits numériques :

« L'intégration de la gestion des droits numériques (DRM) dans *Windows* implique que la société *Microsoft* peut à tout moment révoquer votre droit d'accès aux contenus sécurisés si elle considère votre logiciel compatible-DRM compromis. Une liste de logiciels révoqués est automatiquement installée sur votre ordinateur à chaque téléchargement de contenus sécurisés. Une mise à jour de votre logiciel compatible-DRM est alors nécessaire pour continuer à accéder à vos fichiers sécurisés. Cette révocation n'empêche cependant pas l'accès à des contenus non protégés par les DRM. »

De tels projets constituent effectivement une menace contre la liberté d'expression, et contre les libertés publiques en général. Les entreprises qui les fomentent exploitent abusivement pour leur promotion la psychose de sécurité consécutive au 11 septembre 2001. La puissance de ces entreprises semble considérable, mais nous pensons qu'elles seront néanmoins impuissantes à endiguer les nouvelles pratiques culturelles, parce que celles-ci sont déjà le fait de plusieurs dizaines de millions d'internautes de par le monde, qu'il s'agisse de la publication et de l'échange sur Internet ou du recours aux logiciels libres.

Mesures de rétorsion contre les échanges de données

Le gouvernement français a demandé à Antoine Brugidou, d'*Accenture*, et à Gilles Kahn, alors président de l'INRIA, un rapport (disponible en ligne) sur les échanges de fichiers musicaux par Internet et sur les moyens éventuels de les contrôler ou de les bloquer par des dispositifs techniques[10]. Ce rapport est destiné notamment à répondre aux préoccupations des syndicats français des entreprises de l'édition phonographique et cinématographique, qui ne pensent qu'à interdire, détecter, bloquer et punir les échanges en question.

La réponse donnée par le rapport est que les mesures techniques de contrôle et d'interdiction dont rêvent les éditeurs seront difficiles à mettre en œuvre, très coûteuses, et d'une efficacité limitée dans le temps. En effet les systèmes de filtrage de flux sur l'Internet, pour être réellement efficaces, devraient être installés au cœur

[9] http://www.adullact.org/documents/comparatif_licences.html
[10] http://www.recherche.gouv.fr/discours/2005/musiqueinternet.htm

des réseaux des fournisseurs d'accès à l'Internet (FAI) ; or les FAI ne manifestent aucun enthousiasme à l'idée d'encombrer leurs infrastructures avec ces matériels onéreux, qui vont ralentir le débit de leurs réseaux, et dont l'objectif est d'empêcher leurs clients de se livrer aux activités pour lesquelles justement ils ont souscrit un abonnement à haut débit. Si le ministère de la Culture soutient les syndicats d'éditeurs, le ministère de l'Industrie soutient les FAI.

Les principes de fonctionnement des dispositifs de filtrage ne sont pas déterministes, mais heuristiques : en effet rien ne permet de distinguer de façon sûre un échange poste à poste « suspect » d'un autre type de trafic, comme nous l'avons vu à la page 210. Le filtrage des adresses IP, des numéros de ports ou d'autres données de protocole sont totalement inefficaces contre ce type de trafic. Les systèmes de détection doivent donc reconnaître la « signature » d'un échange, puis ouvrir les paquets pour en investiguer le contenu et mettre en évidence le « délit ». Chaque fois que le protocole (non public) du système poste à poste sera modifié, les systèmes de détection seront mis en échec.

Les sociétés *Allot* et *Cisco* (gamme *P_Cube*) proposent des solutions de filtrage de protocole basés sur la reconnaissance de signature. Les sociétés *Audible Magic* (boîtier *CopySense*) et *Advestigo* proposent du filtrage de contenus. Il y a aussi des systèmes de filtrage sur le poste client, qui supposent la collaboration de l'utilisateur, par exemple dans le cas de parents qui souhaitent empêcher leurs enfants de s'adonner au téléchargement ; cet état de fait pourrait changer avec des dispositifs tels que TCPA (cf. page 235) et NGSCB (cf. page 236), susceptibles d'être utilisés pour surveiller un ordinateur sans le consentement de son propriétaire légitime, mais nous voulons croire que des situations aussi iniques ne pourront pas voir le jour.

MM. Brugidou et Kahn envisagent dans leur rapport plusieurs scénarios de déploiement d'outils de filtrage sur les infrastructures des FAI. Ces équipements, pour jouer leur rôle, devront être installés en coupure, ce qui signifie qu'ils devront être adaptés au débit des infrastructures, soit aujourd'hui généralement 1 gigabit/s, mais bientôt 10 Gb/s, c'est-à-dire qu'ils seront coûteux. Ainsi, le rapport envisage une solution suggérée par un syndicat professionnel et adaptée au réseau de France Télécom : elle consisterait à implanter un boîtier *Allot* à 1 Gb/s en coupure derrière chaque BAS *(Broadband Access Server)* du réseau ADSL de l'opérateur, soit à l'époque de l'étude 143 boîtiers. Le prix de chaque boîtier est de plusieurs dizaines de milliers d'euros. Les fournisseurs d'accès à l'Internet n'ont

guère d'attrait pour ce type d'investissement, qui pénaliserait surtout leurs clients en termes de performances du réseau et de liberté d'usage de leurs ordinateurs, et ce pour une efficacité très discutable.

VOCABULAIRE BAS et DSLAM

Les accès ADSL *(Asymmetric Digital Subscriber Line)* d'un opérateur sont raccordés à un DSLAM *(DSL Access Multiplexer)*. Un DSLAM sera en général installé dans un central (nommé désormais *Nœud de Raccordement d'Abonné,* ou NRA) et desservira une zone de 4 ou 5 km de rayon. Un BAS concentrera le trafic d'une dizaine de DSLAM.

La voie du blocage des échanges de fichiers sur le réseau semble donc peu prometteuse pour les industriels de la culture : on comprend qu'ils soient tentés de se rabattre sur l'implantation de la gestion numérique des droits au cœur de l'ordinateur, avec des technologies telles que les TPM (cf. page 235) et NGSCB (cf. page 236). Ces dernières solutions pourraient être techniquement efficaces, mais elles seraient inacceptables pour les utilisateurs, qui y verraient un empiètement intolérable sur leur liberté d'utiliser comme bon leur semble les objets et les supports numériques qu'ils ont achetés.

Gestion des droits numériques (DRM) et politique publique

Dans un article des *Communications of the ACM (CACM)* de juillet 2005[11], Edward W. Felten, professeur d'informatique et de politique publique à l'université de Princeton, où il dirige en outre le *Center for Information Technology Policy*, a proposé aux instigateurs et aux auteurs de politiques publiques pour la gestion des droits numériques six principes qui lui semblent s'imposer :

- **Pluralité et concurrence :** une politique publique des droits numériques devrait permettre la pluralité des systèmes de gestion de droits, et promouvoir l'interopérabilité entre ces systèmes.
- **Équilibre du droit d'auteur :** les législations relatives au droit d'auteur ont, traditionnellement, cherché un équilibre entre la rémunération de l'auteur et le droit d'accès du public ; la gestion des droits numériques et les législations qui s'y appliquent devraient respecter cet équilibre, non le remettre en cause.

[11] Cf. `http://www.csl.sri.com/users/neumann/insiderisks05.html#181`

- **Protection du consommateur :** les systèmes de gestion des droits numériques ne devraient pas restreindre les droits des consommateurs, et les politiques publiques qui s'y appliquent devraient les protéger.
- **Protection de la vie privée :** les politiques publiques relatives à la gestion des droits numériques devront veiller à la protection de la vie privée, en empêchant que les systèmes de gestion de ces droits ne deviennent des moyens d'espionner les utilisateurs en recueillant des données sur leurs comportements et leurs pratiques culturelles ou autres.
- **Recherche et débat public :** la politique publique devra favoriser la recherche et le débat public sur les questions relatives aux droits numériques, et faire obstacle aux dérives récentes, qui ont vu certaines entreprises tenter d'utiliser les législations sur la propriété intellectuelle pour assigner en justice des auteurs d'articles scientifiques ou de logiciels de recherche.
- **Délimitation du champ d'application :** les politiques publiques devront voir leur champ d'application délimité précisément au domaine où elles seront utiles, et éviter les formulations susceptibles d'être détournées par des avocats trop habiles à l'encontre d'usages légitimes des droits numériques.

Ces principes équilibrés devraient pouvoir recueillir l'assentiment de tous les interlocuteurs de bonne foi dans le débat. Si la gestion des droits numériques devait devenir soit, pour l'industrie culturelle, un moyen de tondre plus efficacement un consommateur sans défense, soit, pour une mouvance libertaire extrémiste, un moyen de profiter des œuvres d'art sans rémunérer les artistes, elle serait de toutes les façons condamnée à l'échec ; nous croyons que ces deux voies extrêmes n'ont aucun avenir.