Les systèmes sécurisés

MARK STEFIK

La mise en place de dispositifs de protection numérique des droits d'auteur permettra aux auteurs de publier sereinement leurs œuvres sur l'Internet.

La banalisation de l'informatique a rapidement conduit les utilisateurs d'ordinateurs à penser que toutes les œuvres numériques – les programmes informatiques, les livres, les revues, la musique et la vidéo – pouvaient être copiées. Certaines figures de l'informatique ont même proclamé que la simplicité de la reproduction marquait la fin des droits d'auteur : «l'information veut être libre», disaient-ils. Autrement dit, il serait impossible de s'opposer à la diffusion de l'information, et tout ce qui peut s'exprimer sous forme de bits pourrait être impunément reproduit.

Cette idée est à la base de la création du réseau Internet : dans la nouvelle ère numérique où nous entrons, l'accès à l'information numérisée serait universel, et l'œuvre de n'importe quel auteur devrait être accessible à n'importe qui, n'importe où et n'importe quand.

Toutefois, par expérience, les utilisateurs du réseau savent que ce dernier ne contient pas de grandes œuvres ni d'informations capitales ; ce qu'on y trouve est souvent de faible valeur. La raison en est que les auteurs ou les éditeurs ne peuvent vivre en faisant cadeau de leur travail. Il suffit aujourd'hui de taper quelques touches d'un clavier pour copier un paragraphe, une revue, un livre, voire l'œuvre d'une vie. La duplication incontrôlée a tant modifié l'équilibre du contrat social entre les créateurs et les consommateurs d'œuvres numériques que la plupart des éditeurs et des auteurs refusent de laisser circuler le meilleur de leurs travaux sous forme numérique.

Toutefois, en coulisse, la technique se prépare à modifier cet équilibre. Au cours des toutes dernières années, plusieurs sociétés, telles *Folio*, *IBM*, *Intertrust*, *NetRights*, *Xerox* ou *Wave Systems*, ont mis au point des programmes et des

Jeff Brice

machines qui permettent aux éditeurs de spécifier les modalités d'utilisation des œuvres numériques et de contrôler leur utilisation. Certains législateurs pensent que ce changement est si radical que les éditeurs auront un pouvoir excessif, et que les consommateurs et les bibliothécaires seront lésés.

Pourtant les besoins des consommateurs seront satisfaits, même avec les nouveaux systèmes : la technique introduisant davantage de sécurité, des œuvres de meilleure qualité pourront être proposées sur le réseau. Bien protégés, des auteurs célèbres auront peut-être envie de publier directement sur le réseau. L'accès à l'information ne sera peut-être pas gratuit, mais il pourrait être bien moins onéreux qu'aujourd'hui, car les coûts d'impression et de distribution sont considérablement réduits par la mise des informations sur le réseau ; les éditeurs pourraient répercuter ces économies aux consommateurs.

Les systèmes «sécurisés» sont la clé de cette mutation technique : ce sont des machines et des programmes dont le fonctionnement se conforme à des règles, nommées droits d'usage, qui définissent le coût d'accès aux œuvres numérisées et les modalités de leur utilisation. Un ordinateur sécurisé, par exemple, refuserait de faire des copies non autorisées ou de transmettre des documents sonores ou graphiques à un utilisateur qui n'aurait pas payé pour les acquérir.

Les types de systèmes sécurisés sont variés : des lecteurs sécurisés peuvent lire des livres numérisés, des magnétophones et des magnétoscopes sécurisés peuvent lire des enregistrements audio et vidéo, des imprimantes sécurisées peuvent faire des copies contenant des signes (des «filigranes») qui indiquent le droit d'utilisation et de reproduction accordé, et des serveurs sécurisés peuvent se charger de vendre des œuvres numériques sur l'Internet. Bien que complexes, les techniques d'élaboration des systèmes sécurisés ont une fonction simple : elles permettent aux éditeurs de distribuer leurs produits – sous forme cryptée –, de sorte que ceux-ci ne soient affichés ou imprimés que par des machines sécurisées. Les premiers systèmes sécurisés équiperaient des imprimantes ou des lecteurs numériques de poche – avec un surcoût pour l'utilisateur, qui accéderait alors à des documents bien plus intéressants qu'aujourd'hui. Puis, comme toujours, l'avènement des nouvelles techniques en ferait chuter les prix. Naturellement les éditeurs pourront encore donner gratuitement l'accès à certaines œuvres : les serveurs sécurisés les transmettront alors sans imposer les protocoles spécifiques des œuvres protégées.

Comment les systèmes sécurisés savent-ils les règles qui doivent être respectées ? La Société *Xerox* et d'autres ont tenté de décrire les montants des droits et les modalités précises d'utilisation dans un langage formel qui sera interprété par les systèmes sécurisés. Le recours à un tel langage est essentiel pour l'édition électronique : les vendeurs et les acheteurs ne pourront négocier et parvenir à des accords que si l'ensemble des actions autorisées ou interdites est explicitement défini. Les droits numériques sont de plusieurs types. Les droits de transport concer-

nent l'autorisation de copier, de transférer ou de charger. Les droits d'interprétation concernent l'autorisation de jouer et d'imprimer. Les droits de reproduction concernent l'extraction d'information, l'édition de cette information et son insertion dans d'autres publications. D'autres droits régissent la création et l'utilisation des copies de sauvegarde.

La sécurisation à l'œuvre

Les exigences de sécurité variant avec la nature des œuvres intellectuelles, les systèmes sécurisés permettent aux éditeurs de définir le degré de maîtrise qu'ils veulent conserver sur les documents écrits, sonores ou vidéo. Les œuvres numériques les plus précieuses peuvent être protégées par des systèmes qui détectent toute tentative de déverrouillage, déclenchent alors des alarmes et effacent l'information abusivement utilisée. À un niveau inférieur, les systèmes sécurisés pourraient seulement éviter les tentatives d'effraction banales en demandant un mot de passe. À un niveau encore plus élémentaire, ils marqueraient seulement les œuvres d'une signature numérique, de sorte le propriétaire soit associé à son œuvre de façon indélébile (certains logiciels de manipulation d'images apposent déjà ce type de filigrane numérique).

La plupart des ordinateurs sécurisés savent reconnaître un autre système sécurisé, faire respecter les droits d'usage et présenter les œuvres de sorte qu'elles ne puissent être copiées exactement ou qu'elles contiennent constamment la marque de leur origine. Pour exécuter les transactions en toute sécurité, deux systèmes sécurisés utilisent un canal de communications, tel le réseau Internet, pour s'échanger des preuves de leurs identités. On peut ensuite gérer les communications sur un canal sécurisé à l'aide d'un cryptage et de ce que l'on nomme un protocole d'authentification.

Par exemple, si un ordinateur *A* veut communiquer avec un ordinateur *B*, il doit prouver à *B* qu'il est un système sécurisé et que son identité est bien celle qu'il déclare sienne. L'interaction commence alors par l'envoi, de *A* à *B*, d'un certificat numérique qui confirme qu'il est enregistré en tant que système sécurisé. L'ordinateur *B* déchiffre alors ce certificat, mais il doit s'assurer que *A* est bien celui que le certificat atteste, et qu'il n'utilise pas frauduleusement un certificat volé : aussi, l'ordinateur *B* compose une chaîne de nombres aléatoires, qu'il chiffre à l'aide d'une clé publique contenue dans le certificat numérique envoyé par *A*. La clé publique permet à *B* d'envoyer des messages que seul *A* comprend lorsqu'il les déchiffre avec sa propre clé.

A doit ainsi déchiffrer le message renvoyé par *B* et retourner un message non chiffré contenant la chaîne aléatoire sélectionnée. Si la chaîne renvoyée en clair est bien celle qui avait été envoyée par *B*, ce dernier sait qu'il est en communication avec *A*, car seul *A* pouvait déchiffrer le message avec sa clé privée. Quelques étapes supplémentaires permettent ensuite aux deux ordinateurs d'effectuer la transaction prévue, telle que le transfert d'un livre sous une forme numérique.

Les systèmes sécurisés n'utilisent pas tous un protocole d'authentification, mais la plupart échangent des œuvres sous une forme cryptée. Ils peuvent aussi comporter d'autres systèmes de sécurité : des horloges infalsifiables qui empêchent un utilisateur d'exercer des droits périmés ; des mémoires inviolables qui enregistrent les opérations financières ; des connexions permanentes avec un bureau central lors des transactions.

Les systèmes sécurisés peuvent placer des filigranes d'identification qui permettront de localiser des copies ou des modifications non autorisées. Ces filigranes enregistrent la désignation de l'œuvre, le nom de l'acheteur et le code des appareils sur lesquels l'œuvre est utilisée. Dissimulée dans les blancs d'un texte, une telle information ne gênerait pas les utilisateurs honnêtes, mais elle ne pourrait être effacée par les fraudeurs.

Les éditeurs devraient continuer à surveiller la diffusion non autorisée de leurs œuvres, car on pourra toujours photocopier une page que l'on aura imprimée, ou filmer un écran d'ordinateur à l'aide d'une caméra vidéo. En revanche, les systèmes sécurisés empêchent la diffusion à grande échelle de copies parfaites des originaux numériques. En outre, certains filigranes permettront de suivre à la trace les copies piratées.

Grâce à ces systèmes, les pratiques commerciales de l'édition numérique ne devraient guère différer de celles de la diffusion des œuvres imprimées. Supposez que Christian veuille acheter un livre numérique proposé par un éditeur du réseau Internet. La copie du livre résulte d'une transaction entre le système du vendeur et l'ordinateur de Christian ; lors de la transaction, Christian doit notamment utiliser sa carte de crédit ou son argent numérique pour payer l'exemplaire du livre qu'il lira sur son ordi-

Virgin Records, Jason Goltz

1. ÉCOUTEZ AVANT D'ACHETER! Cette technique de vente pratiquée dans les magasins de disques pourrait apparaître sur le réseau Internet, grâce aux systèmes sécurisés, qui permettent de «tester» les œuvres numériques avant de les acheter.