Est-ce risqué d'acheter en ligne ?

Est-il plus risqué d'acheter sur l'Internet que de faire un achat par Minitel ou par téléphone ? Lorsque l'on achète sur l'Internet, le site propose en général plusieurs options.

Si le site n'est pas sécurisé (le navigateur prévient l'internaute lorsqu'il passe sur un site sécurisé), on vous proposera le plus souvent d'imprimer le bon de commande et de l'envoyer par fax ou par la poste, ce qui revient à un achat par correspondance, dont on ne discutera pas le sécurité.

Parfois, on vous proposera d'entrer votre numéro de carte de crédit en clair. Évitez de le faire, car même si, à l'instar du téléphone, tout le monde n'est pas sur écoute, il existe de logiciels conçus pour enregistrer les messages qui transitent sur le réseau et qui repèrent les suites de 16 chiffres, tels les numéros de carte de crédit. Ainsi, on a saisi des listes de millions de numéros de cartes de crédit chez des pirates américains.

Lorsque le site est sécurisé, le chiffrement dépend du lieu de la boutique et de l'endroit où vous êtes. S'il s'agit d'une boutique américaine, telle la librairie en ligne Amazon.com, la sécurisation théorique est SSL 128 bits. Toutefois, si vous êtes en France, le navigateur que vous utilisez sera bridé en 40 bits, le temps que les navigateurs acceptant plus apparaissent, ou en 56 bits, car, jusqu'à présent, le gouvernement américain refusait l'exportation de logiciels de cryptographie avec une clé secrète plus longue que 56 bits. Si la boutique est en France, vous aurez vraisemblablement affaire à un chiffrement SSL 40 bits.

Le chiffrement SSL avec une clé de 40 bits est-il sûr ? En juillet 1994, un informaticien lança un défi : pouvait-on facilement percer un message chiffré par ce système. Un informaticien français, Damien Doligez, de l'Institut national de recherche en informatique et automatique (INRIA), explora toutes les clés possibles et décrypta le message après huit jours de calculs sur différents ordinateurs dont il disposait, dont des machines parallèles. Aujourd'hui, la vitesse de calcul des ordinateurs a considérablement cru et on obtiendrait le même résultat avec des ordinateurs à base de *Pentium* (PC) ou de *PowerPc* (Mac), facilement disponibles. Cela signifie-t-il qu'il faut avoir peur de mettre son numéro de carte de crédit en ligne ? Le risque est faible, car quel pirate passerait des jours à décrypter un message pour obtenir un numéro de carte de crédit alors que des facturettes de cartes de crédit traînent dans les magasins ?

Quand des systèmes de cryptographie avec des clés secrètes de 128 bits seront disponibles en France et en Europe, ce risque minime n'existera plus : même avec les ordinateurs les plus puissants au monde, des messages chiffrés à l'aide de systèmes tels que PGP, nécessiteraient des années pour être percés.

Ainsi, pour *TRANZIX*, la notion de valeur représente tout objet virtuel ayant une valeur non intrinsèque quelconque, donc tout document numérique valant quelque chose pour quelqu'un. Ces documents incluent les billets virtuels, les certificats numériques, les attestations électroniques (diplômes d'études, preuves d'achat ou de vente, etc.), les moyens d'identification (carte santé, permis de conduire, passeport, etc.)...

TRANZIX généralise non seulement la notion de valeur, mais aussi l'opération de paiement. Ainsi, une valeur peut être transportée du lieu *A* au lieu *B* sans que cette valeur change de possesseur. Elle peut être transférée de *B* à *C*, non seulement en changeant d'endroit – par transport –, mais en changeant aussi de possesseur. Enfin, elle peut être échangée, lors d'une même transaction, contre d'autres valeurs ; la notion d'échange implique donc deux transferts, lors d'une même transaction. Par exemple, *TRANZIX* permet à un usager de transporter une autorisation électronique de chez lui à son bureau, de transférer cette autorisation à son employé afin d'ouvrir une porte ou d'accéder à une imprimante.

Le système utilise des billets numériques personnalisés à l'aide de signatures manuscrites des clients. Un prototype mis au point par notre laboratoire a été utilisé pour des microfacturations. Ce prototype permet de facturer l'utilisation des ressources physiques sur un réseau local (notamment l'impression des documents à l'aide de jetons numériques distribués de manière centralisée) et de facturer l'accès à des ressources virtuelles sur l'Internet (pour l'achat d'informations contenues dans des pages Web, par exemple, à l'aide de billets virtuels prépayés).

Le système assure un niveau de sécurité très élevé, obtenu grâce à un chiffrement asymétrique (deux clés de chiffrement complémentaires sont utilisées ; voir *Cryptographie et réseau*, page 38). De surcroît, la granularité est réglable. C'est une solution exclusivement logicielle, où les utilisateurs peuvent acheter ou vendre en ligne ou hors ligne à l'aide d'un même portefeuille virtuel.

En pratique, comment s'effectue une transaction ? Après avoir acheté des billets numériques, l'acheteur active son portefeuille virtuel en suivant un lien hypertexte payant dans un magasin virtuel. Le portefeuille virtuel du vendeur contacte alors celui de l'acheteur en lui envoyant une requête de paiement pour la marchandise demandée *(voir la figure 2)*. Une fois le paiement approuvé par l'acheteur, un ou plusieurs billets numériques sont envoyés au vendeur, qui peut les déposer immédiatement à la banque afin de vérifier leur validité, prévenant ainsi toute tentative de dépenses multiples.

Le vendeur peut aussi choisir d'effectuer des transactions hors ligne, afin d'augmenter la vitesse de traitement pour les microtransactions, par exemple ; les billets sont alors déposés par lots à la banque à la fin de la journée ou de la semaine. De cette manière, en réduisant les coûts de traitement des transactions, tant pour les vendeurs que pour les banques, *TRANZIX* rend économiquement viables les microtransactions.

Tout comme dans le monde réel, où plusieurs systèmes de paiement coexistent, plusieurs moyens de paiement numérique seront présents dans le portefeuille virtuel du consommateur de demain. En définitive, les consommateurs décideront quels moyens transactionnels répondent le mieux à leurs besoins spécifiques et quels types de systèmes particuliers survivront dans l'économie virtuelle du futur.

Octavian URECHE prépare sa thèse de doctorat au laboratoire SCRIBENS de l'École polytechnique de Montréal dont Réjean PLAMONDON est le directeur.

O. URECHE et R. PLAMONDON, *Document Transport, Transfer and Exchange : Security and Commercial Aspects*, 5th International Conference on Document Analysis and Recognition, in *IEEE Computer Society*, Bangalore, 1999.

O. URECHE et R. PLAMONDON, *Système électronique de transfert numérique de valeur : étude de faisabilité*, École polytechnique de Montréal, EPM / RT-96 / 22, 1996.

Pour la libéralisation de la cryptographie

RONALD RIVEST

L'un des pionniers de la sécurité informatique s'oppose au contrôle gouvernemental de la cryptographie.

Le développement de la cryptographie est une conséquence inéluctable de la révolution informatique. Avec l'apparition des communications entre les ordinateurs, les utilisateurs cherchent à sécuriser les conversations et les transactions. La cryptographie est la… clé de cette sécurisation, mais sa généralisation est débattue. Aux États-Unis, le gouvernement veut restreindre l'usage de la cryptographie, car il craint que les criminels et les espions ne l'utilisent.

Avant 1970, la cryptographie était trop compliquée et trop onéreuse pour un usage courant. Grâce à deux inventions – la cryptographie à clé publique et le microprocesseur –, les méthodes cryptographiques sont devenues si performantes qu'il faudrait des années de calcul sur ordinateur pour décoder un message dont on ignore la clé. Les ordinateurs capables d'exécuter ces méthodes sont devenus largement accessibles.

Toutefois, vers la fin des années 1980, lorsqu'une cryptographie civile devint ainsi possible, deux agences américaines s'inquiétèrent de sa généralisation. L'Agence de sécurité américaine (NSA, soit *National Security Agency*), qui surveille les communications électroniques mondiales, s'alarma de ne plus pouvoir décrypter les messages chiffrés d'espions ou de terroristes potentiels. D'autre part, le FBI craignit que les criminels n'usent de logiciels de cryptographie pour déjouer la surveillance de leurs communications. Durant la dernière décennie, ces organismes ont poussé le gouvernement américain à réglementer l'usage de la cryptographie et à limiter l'exportation de logiciels de cryptographie performants.

Doit-on priver l'ensemble des utilisateurs de techniques, sous prétexte que quelques criminels pourraient les utiliser à leur avantage? L'argument est spécieux : on n'empêche pas le public d'acheter des gants sous prétexte que les voleurs en utilisent pour éviter de laisser des empreintes digitales. Restons sur ce dernier exemple.

La cryptographie protège les données ; les gants protègent les mains. La cryptographie protège contre les intrus et les espions industriels ; les gants protègent contre les coupures, la chaleur, le froid et les infections. La cryptographie peut gêner la police, qui ne pourra plus pratiquer d'écoutes téléphoniques ; les gants peuvent gêner la police qui trouve difficilement des empreintes digitales. La cryptographie est devenue bon marché et d'emploi facile ; les gants le sont depuis longtemps. Enfin, on peut télécharger des logiciels de cryptographie à partir du réseau Internet pour un coût inférieur à celui d'une bonne paire de gants.

Le travail de la police deviendra certainement plus difficile si tous les utilisateurs du réseau chiffrent leurs échanges, mais nous ne sortirons correctement de ce dilemme que si nous pesons les avantages et les inconvénients collectifs de l'innovation. La plupart des utilisateurs envisagent d'utiliser la cryptographie pour prévenir les crimes plutôt que pour les cacher, comme ils utilisent les gants pour protéger leurs mains plutôt que pour dissimuler leurs empreintes. En assurant la confidentialité et l'authentification des opérations bancaires et commerciales, la cryptographie empêche le vol et la fraude aux cartes de crédit, et elle évite le piratage industriel. Paradoxalement, on créera une société plus sûre si l'on adopte une technique qui entrave quelque peu l'application des lois.

Certains ont souhaité un compromis qui généraliserait les systèmes cryptographiques élaborés en permettant aux États de déchiffrer les messages en cas de besoin : par exemple, on pourrait demander aux utilisateurs d'enregistrer leurs clés de chiffrement auprès d'organismes assermentés ou de donner aux autorités des moyens secrets d'accéder à ces clés. Une version cryptée de la clé qui a chiffré le message serait envoyée en même temps que celui-ci. Un centre de recouvrement des clés pourrait utiliser une super clé secrète pour déchiffrer la clé, puis déchiffrer le message lui-même.