Pour la libéralisation du chiffrement en France (publié dans Le Monde)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 février 1995. Dernière mise à jour le 17 décembre 2014

https://www.bortzmeyer.org/crypto.html

Cet article avait été publié dans le quotidien Le Monde en 1995. Sauf erreur, c'était le premier article en France à critiquer publiquement la quasi-interdiction de la cryptographie qui existait à l'époque (elle a été partiellement libéralisée par la suite avec le décret n°2001-1192 du 13 décembre 2001 et la loi n°2004-575 du 21 juin 2004).

Il y avait en effet beaucoup de FUD en France à l'époque concernant la législation sur la cryptographie, le SCSSI et les autres services gouvernementaux essayant de brouiller la situation pour ne pas indiquer que la France était le pire pays du monde occidental en ce qui concerne les restrictions à l'usage de la crypto. Bien sûr, tout le monde s'en moquait depuis des années et les services gouvernementaux n'étaient pas les derniers à échanger des messages chiffrés en PGP (sans que leurs correspondants se retrouvent en prison) mais cette épée de Damoclès permanente pesait lourdement sur l'utilisation du chiffrement. Merci donc à Edwy Plenel pour avoir permis la publication de cet article à l'époque et merci à Amaelle Guiton pour avoir trouvé une version déjà numérisée. Voici le texte intégral :

La communication entre citoyens, aujourd'hui, se fait de plus en plus par le truchement de réseaux complexes, que l'individu ne peut totalement contrôler. Que ce soit le téléphone, la télécopie, ou de plus en plus les réseaux informatiques comme Internet, on ne peut pas avoir confiance dans ce qui se passe sur le réseau. On ne peut pas être sûr que les messages ne seront pas écoutés, on n'a aucune garantie qu'ils arriveront non déformés, on n'a pas de preuve de l'identité de l'expéditeur.

Les techniques modernes remettent en cause bien des certitudes : la manipulation d'un message, même vocal, l'écoute "en grand" par des ordinateurs et non pas par des personnes, en nombre forcément limité, donnent aux malhonnêtes ou à ceux qui abusent de leur pouvoir des armes redoutables.

Bien sûr, il existe des lois. Les écoutes téléphoniques sont réglementées. Elle ne peuvent être effectuées que dans des conditions bien précises, et à seule fin de lutter contre le crime. En l'absence de toute jurisprudence, on peut penser que ces lois s'appliquent également aux réseaux informatiques.

Mais la mise en examen de plusieurs membres de la fameuse "cellule de l'Élysée" en décembre 1994 dans l'affaire dite des écoutes téléphoniques de l'Élysée illustre la faiblesse de la protection donnée par la loi. Face aux outils modernes et aux moyens qu'ils offrent (et qu'ils offriront de plus en plus) à ceux qui veulent violer la loi et les droits du citoyen, il est nécessaire de permettre à celui-ci d'utiliser la technique pour se protéger. Je considère en effet qu'un citoyen a droit à sa vie privée et qu'il peut souhaiter dissimuler le contenu de ses messages sans avoir de compte à rendre.

Il n'existe aucun moyen de garantir une sécurité complète sur un réseau, qu'il soit téléphonique ou informatique. Les messages peuvent être écoutés par des gouvernements peu scrupuleux, par un employé indélicat, par n'importe qui s'il se branche sur l'un des endroits vulnérables du réseau. La complexité de plus en plus grandes des réseaux, leur internationalisation, peut-être demain leur privatisation, rendra de plus en plus difficile toute protection basée sur la confiance dans la compagnie qui gère le réseau. Non seulement cette vulnérabilité est une menace pour les droits du citoyen (parmi lesquels figurent le droit à la vie privée) mais c'est aussi une gêne pour la vie économique. De plus en plus d'entreprises vont utiliser ces réseaux de communication et la sécurité des messages, par exemple pour les paiements électroniques, est une question sérieuse.

Il existe une solution technique à ce problème de la confidentialité, (ainsi d'ailleurs qu'à ceux du contrôle de l'intégrité des messages échangés et de l'authentification de l'expéditeur). Elle est basée sur les techniques de cryptographie.

La cryptographie est l'ensemble des moyens permettant de chiffrer, de rendre incompréhensible un message. Une fois cette opération effectuée, le message peut emprunter n'importe quel type de réseau, public ou privé, français ou étranger sans risque. Sur le trajet, une grande oreille peu scrupuleuse pourra lire le message ; elle ne pourra pas le déchiffrer.

Les techniques de chiffrement ont connu de grands développements depuis vingt ans. La cryptographie dite "à clé publique" permet d'envoyer un message de façon fiable à quelqu'un sans avoir eu à échanger une clé secrète précédemment. La "signature électronique" et le "résumé de message" rendent possible l'authentification du message et garantissent qu'il n'a pas été modifié en cours de route. Enfin, des logiciels mettant en oeuvre ces techniques de façon efficace sont maintenant disponibles, parfois gratuitement comme le programme PGP ("Pretty Good Privacy"), devenu la norme de fait en matière de chiffrement, permettant ainsi à tous de communiquer de façon sûre.

Alors, quel est le problème puisque la technique résout tout ?

Le problème est que l'utilisation des techniques cryptographiques en France reste interdite, ou plus précisément réservée aux militaires, policiers et, dans une certaine mesure, banquiers. Le simple citoyen, l'association, l'université ou la petite entreprise en sont exclus.

Ces techniques sont interdites par la loi 90-1170 du 29 décembre 1990 qui soumet l'utilisation de toute technique de chiffrement en France à une autorisation. Ces autorisations sont délivrées par le Service Central pour la Sécurité des Systèmes d'Information (SCSSI) qui dépend directement du Premier Ministre (pendant la guerre froide, il dépendait de l'Armée). Les critères d'autorisation ou de refus du SCSSI sont secrets. Cet organisme ne publie pas de rapport d'activité.

Il semble (on en est réduit aux déductions puisque le SCSSI ne publie pas ses principes de choix) que la politique d'autorisation soit la suivante : l'organisation qui demande doit fournir la preuve que le système de chiffrement qu'elle utilise est suffisamment peu fiable pour qu'un écoutant disposant de moyens importants puisse "casser" son code, le déchiffrer. Les logiciels trop efficaces, c'est-à-dire trop

difficiles à casser, comme PGP, sont de fait interdits. En tout état de cause, seule l'organisation dont les besoins de sécurité sont jugés dignes d'intérêt par le SCSSI peut espérer avoir une autorisation.

Pourquoi cette loi et cette pratique ? L'argument le plus souvent donné est que les écoutes ("interceptions") sont nécessaires à la lutte contre le crime. Si chacun pouvait chiffrer ses transmissions, un outil d'enquête efficace deviendrait difficilement utilisable.

Cette argumentation n'est pas satisfaisante pour plusieurs raisons. D'abord, elle pose comme postulat que les écoutes ne seront utilisés que par les autorités légales et uniquement dans un but de lutte contre le crime. En fait, les exemples ne manquent pas d'écoutes effectuées dans de tout autres buts, ou d'écoutes réalisées par des gens qui n'y étaient pas autorisés, mais qui exploitaient ces failles dans les réseaux mentionnées au début. Si un réseau n'est pas rendu sûr grâce au chiffrement, tout le monde peut y intercepter des messages, aussi bien le policier légalement chargé d'une enquête que le, disons, l'écoutant illégal.

En outre, l'interdiction du chiffrement profite aux criminels puisqu'ils peuvent écouter tranquillement les messages circulant sur les réseaux.

Mais surtout, cette argumentation suppose que la lutte contre le crime justifie tout. Or, tous les progrès des droits du citoyen peuvent potentiellement profiter au criminel. Cela n'a pas empêché ces progrès de se réaliser depuis deux siècles.

Notons enfin que des pays voisins, aux systèmes économiques et sociaux proches, autorisent déjà le chiffrement, ne maintenant de restrictions qu'à l'exportation : Allemagne et Grande-Bretagne par exemple. Or, la criminalité n'y est pas plus élevée qu'en France.

Il est donc nécessaire de corriger cette archaïsme qui consiste à traiter la cryptographie comme une arme ultra-secrète dans un pays en guerre. Le développement de l'utilisation des réseaux ne peut pas se faire sans les techniques de la cryptographie.

[Fin de l'article paru dans le Monde.]

Cet article avait suscité une critique de Joël de Rosnay, à laquelle j'ai répondu dans un article de Libération <http://www.liberation.fr/ecrans/1995/04/06/stephane-bortzmeyer-le-cryptage-est-t
130964>.