Le Projet Emeraude

- Questions de société - Les services de renseignements -

Date de mise en ligne : mercredi 10 novembre 2010

Description :

Jusqu'en 1999, l'usage de la crypto "forte" (c- a- d uti-lisant des clés supé-rieures à 128 bits) était interdit en France pour les par-ti-cu-liers et la majorité des entre-prises. Pourquoi ?

Projet 22

Sommaire

- I) But et Moyens juridiques
- II) Comment Emeraude résout
- III) Comment se défendre (...)

Prologue : La cryptologie en France.

Jusqu'en 1999, l'usage de la crypto "forte" (c- a- d uti-lisant des clés supé-rieures à 128 bits) était interdit en France pour les par-ti-cu-liers et la majorité des entre-prises. Pourquoi ? Selon l'administration, la crypto per-met-trait aux ter-ro-ristes et gang-sters de tout poil de berner les ser-vices chargés de lutter contre eux. Ceci n'empêchait d'ailleurs pas que le logiciel PGP ("Pretty Good Privacy" aux clés com-prises entre 128 et 2048 bits), interdit en France, y soit lar-gement utilisé.

Puis, l'usage de la crypto "forte" a été autorisé pour per-mettre aux entre-prises fran-çaises de se pro-téger contre les inter-cep-tions amé-ri-caines (le réseau Echelon, encore et tou-jours). Tou-tefois, on assiste depuis quelques mois à une impor-tante aug-men-tation du nombre de per-sonnes l'utilisant pour crypter leurs mails (avec un certain nombre de ter-ro-ristes et autres gang-sters dedans).

I) But et Moyens juridiques donnant naissance au projet Emeraude.

Le projet Eme-raude consiste à ins-taller des moyens d'interception de tout trafic ayant pour origine ou des-ti-nation un inter-naute situé sur le ter-ri-toire français. C'est tech-ni-quement très facile, comme en quelque sorte d' ins-taller une "bre-telle" sur une ligne téléphonique.

Le but de ce projet est de "per-mettre aux ser-vices de lutte contre le ter-ro-risme et contre le ban-di-tisme organisé, d'intercepter tout échange de données et d'informations sus-cep-tibles de porter atteinte à l'ordre public ou à la sécurité du ter-ri-toire" selon une note du cabinet du Premier Ministre en date du 3 février 2000.

Juri-di-quement, les choses sont simples : Tout magistrat peut ordonner l'interception des com-mu-ni-ca-tions de toute per-sonne soup-çonnée de quoi que ce soit. Ce sont les écoutes "judi-ciaires". De plus, dans les cas d'atteintes à la sûreté de l'état, on peut aussi ordonner des écoutes "admi-nis-tra-tives" (comme celles ordonnées par exemple par François Mit-terrand contre Carole Bouquet... mdr). Le cadre juri-dique existe donc.

II) Comment Emeraude résout le problème des mails cryptés.

Avec le déve-lop-pement de la crypto "à la portée de tous", le projet Eme-raude avait un gros pro-blème : inter-cepter les emails c'est bien, mais si ceux- ci sont cryptés, ça ne sert pas à grand- chose ! En effet, la DST n'a pas les moyens infor-ma-tiques de la NSA et elle ne pourra pas casser en même temps le code de cen-taines de mil-liers de mails. Tou-tefois une solution simple a été trouvée...

Des constats évidents ont été fait : PGP est qua-siment le seul logiciel de cryptage utilisé par le "grand public" et tout message crypté par PGP com-mence par les mêmes séquences.

Il a donc été décidé, très simplement, deux choses :

- 1) Repérer les sus-pects poten-tiels, c'est à dire tous ceux qui cryptent leur courrier. Dans le lot, il se trouvera bien quelques ter-ro-ristes et gangsters.

- 2) Par ailleurs, "en cas de doute", si on ne peut pas décrypter les données, on les détruit. Les seuls mails cryptés que vous pouvez donc recevoir dans votre mailbox sont donc des mails qui ont été "lus" aupa-ravant par les ordi-na-teurs du Ministère de l'Intérieur...

Comme les ser-vices ne veulent pas passer leur temps à contrôler le courrier, le boulot sera imposé aux four-nis-seurs de service ! C'est d'ailleurs en quelque sorte ce qu'il se passe concernant les écoutes télé-pho-niques, qui sont main-tenant effec-tuées par des agents des télécoms, qui trans-mettent ensuite les bandes aux ser-vices deman-deurs (Sauf en cas d'écoutes "admi-nis-tra-tives", alors gérées direc-tement par le Ministère de la Défense).

Ainsi, les four-nis-seurs d'accès français ont été priés, au mois de mars 2000, de pré-parer un système de contrôle des mails, direc-tement sur leurs ser-veurs. Concrè-tement donc, si vous cryptez votre courrier, vous serez inscrit sur une liste par-ti-cu-lière qui sera transmise au Ministère de l'intérieur (euh...n'oubliez pas que votre four-nisseur sait qui vous êtes, puisqu'il connaît le numéro de télé-phone par lequel vous vous connectez.)

III) Comment se défendre ?

Un moyen de contrer cet espionnage consis-terait à uti-liser un autre logiciel que PGP. Facile pour les pro-fes-sionnels de l'informatique, beaucoup moins pour les ama-teurs. De toutes façon, Eme-raude serait capable depuis mi- 2001 de repérer toutes com-mu-ni-ca-tions cryptées, quelque soit le logiciel utilisé...

Un autre moyen est d'employer des pro-cédés de sté-ga-no-graphie, consis-tants à dis-si-muler au sein de fichiers "anodins" (images, pages html, etc) d'autres fichiers. Cette solution est de loin la plus "sure", car vos fichiers confi-den-tiels peuvent alors être cachés au sein d'une photo de vacances par exemple et le "filtre PGP" ne détectera stric-tement rien.