Les crypto-wars (3/3): «Apple se refait une virginité à peu de frais»

PAR JÉRÔME HOURDEAUX
ARTICLE PUBLIÉ LE MARDI 3 MAI 2016

Pour la chercheuse en cryptologie Anne Canteaut, le débat sur le chiffrement des téléphones et l'installation de « backdoors » *« est biaisé ». « Il n'existe aucun algorithme qui soit sûr dans l'absolu. C'est qu'ils n'ont pas encore été cassés, tout simplement »*, explique-t-elle. Entretien.

Anne Canteaut est chercheuse en cryptologie, directrice de l'**équipe SECRET**, travaillant sur la conception et l'analyse de la sécurité d'algorithmes cryptographiques, au sein de l'Institut national de recherche en informatique et en automatique (Inria). Entretien.

Anne Canteaut est chercheuse en cryptologie.

La justice se trouve-t-elle réellement régulièrement confrontée à des équipements chiffrés qu'elle est incapable de déchiffrer ? Existe-t-il des algorithmes de chiffrement incassables ?

Anne Canteaut. Sur l'ensemble des algorithmes existants, il y en a une quantité qui n'ont pas encore été cassés. Mais cela ne veut pas dire qu'ils sont sûrs. Il n'existe aucun algorithme qui soit sûr dans l'absolu. C'est qu'ils n'ont pas encore été cassés, tout simplement. Il y a tout d'abord les questions de puissance de calcul. La méthode la plus simple consiste à essayer toutes les possibilités pour une clef. Et là, tout dépend des moyens à disposition. Dans le cas d'un téléphone, le plus difficile, ce sera de faire sauter le dispositif limitant le nombre d'essais pour le mot de passe. Une fois ce problème réglé, c'est beaucoup plus simple.

Il y a ensuite la question des capacités d'agences telles que la NSA, ce qu'elles sont capables de faire. Sur ce point, c'est encore moins clair.

Mais surtout, ce débat est biaisé car il se focalise sur un micro-aspect du problème. En fait, c'est assez peu le chiffrement qui est mis en cause dans les attaques, mais davantage tout ce qu'il y a autour du chiffrement. Ces dernières années, les possibilités d'accès aux données ont été démultipliées. Prenons un exemple concret : le protocole HTTPS *[un système de sécurisation de la navigation sur internet. Intégré au navigateur, il permet par exemple de se connecter de manière sécurisée au site de sa banque – ndlr]*. Ce protocole repose sur une mise en relation entre votre navigateur et le serveur du site qui vont négocier sur le type d'algorithme. Une fois qu'ils se sont mis d'accord sur la manière de communiquer, la connexion au site peut se faire. Une des attaques consiste simplement à se faire passer pour un serveur et à contraindre le navigateur à utiliser son algorithme. Dans ce cas, il n'y a même pas besoin de le casser.

Quel est votre sentiment sur le conflit opposant le FBI à Apple ?

Je trouve surtout qu'Apple se refait une virginité à peu de frais ! On a d'ailleurs beaucoup parlé des communications bloquées dans le téléphone de San Bernardino. Mais assez peu du fait qu'elles ne représentaient que cinq jours. Tout le reste avait été synchronisé par les services d'Apple et stockés sur des serveurs. Et là, le FBI y a bien eu accès. Le fait qu'Apple stocke les communications de ses utilisateurs aurait dû tout de même susciter quelques réactions…

Lorsqu'on relit l'histoire du chiffrement, des tentatives de la NSA pour influer sur les standards dès les années 1970 jusqu'aux révélations d'Edward Snowden sur Bullrun, on peut avoir l'impression que la NSA tente systématiquement d'influer secrètement sur les logiciels de chiffrement. Qu'en est-il exactement ?

Faut-il craindre que la plupart des standards aient été équipés de *backdoors* ou pervertis d'une autre manière ?

Pour les *backdoors*, honnêtement, je serais incapable de dire à quel point cette pratique a été appliquée. On sait que la NSA l'a utilisée pour le Dual EC, comme l'ont montré les documents Snowden. Pour le DES *[le premier standard de chiffrement datant de 1977 sur lequel la NSA a fortement pesé. Voir le second volet de notre série – ndlr]*, je serais plus prudente. La NSA est bien intervenue, mais il n'y a pas de certitude.

Les autorités américaines ont eu une influence assez forte sur la diffusion des produits, mais par contre, sur la conception des standards, ce n'est pas clair. La procédure de validation de l'AES *[la norme de chiffrement ayant succédé au DES – ndlr]* a par exemple été totalement différente. Il y a eu un concours mondial, avec 16 candidatures qui ont été étudiées lors de conférences internationales. L'algorithme sélectionné a été développé par des collègues belges, que nous connaissons tous.

Cela dit, ce n'est pas parce qu'il n'y a pas de *backdoors* qu'il n'y a pas des tentatives d'influence. Ainsi, ces dernières années, le NIST tente d'établir un nouveau standard pour un algorithme plus simple et léger destiné à des équipements mobiles, transmettant des informations *via* des puces RFID, par exemple sur votre carte de transports. Il y a deux ans, la NSA a proposé son propre algorithme, SIMON, et pousse depuis pour qu'il soit sélectionné. Bien entendu, la communauté de la cryptologie est plutôt sceptique sur la sécurité de cet algorithme…

Et en France, les chercheurs sont-ils confrontés à ce type de pressions ?

Non, il n'y a pas de situation comparable en France. Nous travaillons avec le ministère de la défense ou l'Anssi. Mais, personnellement, je n'ai jamais subi ni constaté de pression. Je sais que cela n'a pas toujours été le cas. Jusqu'au milieu des années 1990, il y avait des pressions. Mais à ma connaissance, ça a complètement disparu. Toutefois, dans l'ambiance actuelle, les choses peuvent très bien changer. J'imagine, par exemple, qui si nous arrivions à casser l'AES, il faudrait que nous passions un coup de fil à l'Anssi avant de publier nos résultats.

En tant que chercheuse, comment jugez-vous le débat actuel, en France, sur le chiffrement et notamment les propositions visant à obliger les fabricants à instaurer des *backdoors* dans leurs produits ?

Ce que j'entends ces derniers temps est surréaliste. Par mesure de sécurité, on veut supprimer la sécurité ? Ça n'a aucun sens ! C'est comme si, pour faciliter le travail de la police, on décidait d'enlever les portes de toutes les maisons. Ces gens n'ont pas conscience qu'il n'y a pas que les terroristes qui utilisent le chiffrement, mais aussi des responsables politiques, économiques… enfin, je l'espère, et en tout cas ils le devraient !

Je peux comprendre que, dans l'émotion, ce type de solutions paraisse légitime. Mais il faut ensuite réfléchir un peu. On se rend compte alors qu'elles sont surtout dangereuses. C'est une erreur de raisonner en opposant la sécurité du pays et la vie privée. Le chiffrement, ça ne concerne pas que les communications personnelles, mais également la sécurité de notre économie, la sécurité des transmissions de données sensibles… C'est tout cela que l'on affaiblit.

Directeur de la publication : Edwy Plenel
Directeur éditorial : François Bonnet
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 28 501,20€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Gérard Cicurel, Laurent Mauduit, Edwy Plenel (Président), Marie-Hélène Smiéjan, Thierry Wilhelm. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart.
Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 28 501,20€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.