Steve Kremer, Inria : « affaiblir le chiffrement, c'est grotesque »

L'attentat contre le Parlement de Londres semble avoir réveillé les velléités des politiques de mieux encadrer le chiffrement. En mars, la Commission européenne a expliqué vouloir durcir la législation du Vieux Continent en la matière, en obligeant les prestataires de services, comme les messageries chiffrées WhatsApp ou Telegram, à collaborer avec les forces de l'ordre. Une antienne reprise dans le cadre de la campagne présidentielle française par Emmanuel Macron. Dans le cadre d'une conférence de presse en début de semaine, le candidat d'En Marche a clairement pointé la responsabilité des « *grandes compagnies d'Internet* », accusées de refuser de « *communiquer leurs clefs de chiffrement ou de donner accès au contenu* ». Et de lancer que ces entreprises devront « *assumer un jour d'avoir été complices d'attentats* ».

Les modalités d'une collaboration plus active entre les prestataires de services chiffrés et les forces de l'ordre renvoient, très vite, à des questions techniques. Et à une interrogation centrale : peut-on affaiblir le système de chiffrement pour assurer l'accès à l'information de certains – ici, les forces de police – sans affaiblir la sécurité d'ensemble des systèmes ? La réponse de Steve Kremer, directeur de recherche à l'Inria, ne laisse guère de place au doute. Steve Kremer dirige l'équipe de recherche Pesto, spécialisée dans la sécurisation des algorithmes de chiffrement, et il enseigne la théorie de la sécurité.

Silicon.fr : Existe-t-il une solution technique permettant de ménager un accès à des flux chiffrés pour les forces de l'ordre sans (trop) affaiblir la sécurité globale du système ?

Steve Kremer : Cette question, on se la repose régulièrement. Elle a par exemple fleuri aux Etats-Unis dans les années 90 et est revenue sur le devant de la scène tout récemment. Des chercheurs ont étudié le problème et sont parvenus à la conclusion qu'il n'existe aucune solution technique permettant de ménager cet accès sans affaiblir la sécurité globale de façon conséquente. On se trouve ici face à une réelle contradiction.

Regardons les options envisageables. La première solution consisterait à créer une clef maître permettant de déchiffrer tous les échanges. Ce qui est difficile à mettre en œuvre en pratique. Car qui va la détenir ? L'utiliser ? Sous quelles conditions ? Pour des questions de simplicité, les services de sécurité voudront que plusieurs personnes la détiennent. Mais si l'une d'entre elles la perd, c'est l'ensemble de la sécurité du système qui est détruite. Une autre hypothèse consisterait à distribuer cette clef entre plusieurs personnes, qui devraient donc se mettre d'accord pour déchiffrer une communication. Mais, là, le système devient complexe, alors que les forces de sécurité attendent une solution simple.

Et ces solutions affaibliraient de toute façon la sécurité globale des protocoles de chiffrement. Car ceux-ci emploient ce qu'on appelle des clefs de session, utilisées pour un échange unique afin de limiter les risques de compromission. C'est ce que les spécialistes appellent le forward secrecy. Or, si une clef maître est créée, on ne peut plus garantir ce principe.

Si une solution satisfaisante n'existe pas aujourd'hui, peut-on imaginer en concevoir une

demain ?

S.K. : Tous les chercheurs sont unanimes sur un point : pour qu'un système soit sûr, la sécurité doit résider dans la clef et la méthode de chiffrement doit être publique (c'est le principe de Kerckhoffs, formulé… à la fin du XIXème siècle, NDLR). Tout récemment encore, des experts de renommée mondiale, parmi lesquels Ron Rivest (le R de RSA) ou Bruce Schneier, ont collaboré à une étude qui a conclu que des solutions de ce type ne sont pas envisageables et qu'elles ne le seront probablement jamais.

Imaginons même qu'elles le soient : comment va-t-on les mettre en œuvre ? Car une solution de ce type sera par nature plus complexe à implémenter pour les développeurs. Or, on sait par expérience que ces complexités seront la source de nouvelles failles de sécurité. Rappelons-nous que l'affaiblissement du chiffrement par les Etats-Unis – avec des clefs limitées à 512 bits pour les versions destinées à l'export – a des conséquences encore incroyables aujourd'hui sur la sécurité des systèmes (ce qu'ont d'ailleurs très bien montré les travaux de l'Inria sur les failles LogJam ou Freak, NDLR). Dans SSL, une faille permettait de réactiver cette clef faible, qu'on sait aujourd'hui casser à la volée. Ce qui montre que ces solutions laissent des traces, même après avoir essayé de les détricoter !

Par ailleurs, les politiques disent ceci ou cela, mais sans aller très loin dans leurs réflexions. Sans décrire un réel cahier des charges techniques. Telles qu'elles sont décrites, les solutions envisagées sont très, très floues. Certaines déclarations évoquent des travaux sur le sujet, sans qu'on sache à quoi ils font référence…

Dans ses déclarations, la Commissaire européenne à l'origine du futur texte sur le sujet semble pencher pour une collaboration des prestataires, à qui reviendrait la charge de fournir les données demandées par les autorités…

S.K. : Mais comment pourrait-on contrôler pareil dispositif ? S'agit-il de certifier certaines applications, dont les éditeurs se sont engagés à collaborer avec les autorités, et d'interdire les autres ? Ce serait tout simplement grotesque dans un Internet ouvert ! Il n'existe aujourd'hui aucune méthode simple permettant d'interdire certaines applications sur le réseau. Si une législation est votée imposant une modification du chiffrement à WhatsApp ou Telegram (deux messageries pratiquant aujourd'hui le chiffrement de bout en bout, au sein duquel leurs éditeurs n'ont en théorie pas accès aux échanges des utilisateurs, NDLR), des alternatives émergeront. Et un terroriste n'aura aucune réticence à employer une app non certifiée. On le voit, toute législation de ce type sera contre-productive. Ses gains potentiels seront très probablement inférieurs aux pertes et aux risques qu'elle entraînera, par exemple en matière d'espionnage industriel.

A lire aussi :

Affaiblissement du chiffrement et de la neutralité du Net : Tim Berners-Lee s'insurge

L'Europe va proposer une législation affaiblissant le chiffrement

Photo : © Inria / Photo Kaksonen