Science Deux chercheurs Nancéiens du CNRS et de l'INRIA ont mis au jour une faille dans la sécurité d'Internet qui pourrait se révéler intentionnelle. La question de l'espionnage des entreprises est posée

Une faille dans la sécurité d'Internet

Nancy. À qui pourrait profiter une faille dans la sécurité du Net ? « À la NSA par exemple ». Vigie d'Internet au niveau mondial, l'agence de sécurité nationale américaine est citée par Pierrick Gaudry. Chercheur au CNRS, il a mis au jour au sein du laboratoire lorrain de recherche en informatique (Loria), avec Emmanuel Thomé chercheur à l'INRIA et une équipe de chercheurs de l'université de Pennsylvanie, « une faille dans la sécurité d'Internet. Avec l'idée qu'on ne peut pas exclure que la faille que nous avons mise en évidence, ait été créée intentionnellement… ».

De quoi parle-t-on ? Pour communiquer de façon sécurisée, deux ordinateurs mettent en œuvre des protocoles cryptographiques. Une communication chiffrée et totalement invisible pour l'usager lambda. Des algorithmes qui utilisent des nombres premiers (seulement divisibles par un et eux-mêmes). « Ces nombres sont très grands en taille. On parle de 1 024 bits, soit 309 chiffres, au minimum pour pouvoir créer ce que l'on appelle une ''clé" de sécurisation des échanges entre deux ordinateurs », explique Pierrick Gaudry.

« Dans un monde normal, ces nombres n'ont pas de propriétés particulières. Ils sont pris au hasard. Nous avons travaillé à créer un nombre premier qui ait l'air aléatoire. Mais dont la structure arithmétique intérieure cache une porte dérobée ». Porte d'entrée dans la fameuse « clé » de sécurisation d'un échange entre deux ordinateurs. En clair un mouchard, capable de pirater une communication chiffrée en 80 minutes.

■ **Des nombres truqués pour pirater les communications chiffrées entre deux ordinateurs.** Illustration Alexandre MARCHI

Espionnage de réseaux sécurisés d'entreprises

« Si nous avons pu créer cette faille, quelqu'un d'autre a pu le faire. » Car le coup de la porte dérobée n'est pas nouveau. « Nous avons remis au goût du jour une technique créée par un Américain dans les années 90. Ce même chercheur qui a aussitôt été embauché… par la NSA. »

Si l'idée de cette faille avait été jugée « peu crédible » en regard des moyens de l'époque, elle prend une tout autre résonance aujourd'hui. Et pose question.

« On imagine que l'intérêt majeur de ce type de faille intentionnelle n'est pas la surveillance de masse. Mais bien l'espionnage de réseaux sécurisés d'entreprises. On sait qu'aujourd'hui 13 % des réseaux d'entreprise utilisent le même nombre premier ''louche". Qui n'a aucune traçabilité. Et on le retrouve pourtant dans les standards (normes) de sécurisation sur Internet. »

Qui émet des recommandations sur les normes de fabrication des standards de sécurité du Net ? Des instances américaines proches de la NSA. De là à faire le lien avec les révélations du lanceur d'alerte Edward Snowden sur les opérations de surveillance des communications sur Internet par l'agence de sécurité américaine, le pas est franchi.

Et pour monsieur tout le monde ? Cette découverte aura des conséquences positives. « Cette faille fait déjà l'objet de discussions publiques pour faire évoluer les standards de sécurité sur Internet ».

Stéphanie SCHMITT