Des trappes dans plusieurs millions de clés de chiffrement

Des clés de chiffrement de 1024 bits utilisées pour sécuriser les échanges et les communications sur Internet (sites Web, VPN et serveurs), peuvent utiliser des nombres premiers munis de *« trappes »* indétectables. L'exploit permettrait à des pirates de déchiffrer plusieurs millions de communications chiffrées, et d'identifier les propriétaires des clés. C'est ce qui ressort des travaux d'une équipe de chercheurs : Joshua Fried et Nadia Heninger, de l'Université de Pennsylvanie, Emmanuel Thomé et Pierrick Gaudry, de l'équipe projet CARAMBA (Inria-CNRS-Université de Lorraine).

« Nous démontrons dans nos travaux que la création et l'exploitation de trappes des nombres premiers (trapdoored primes) pour les standards d'échange de clés Diffie-Hellman et du DSA (Digital Signature Algorithm) est faisable pour les clés de 1024 bits avec des ressources informatiques universitaires modernes », déclarent les chercheurs dans leur article technique. Ils disent avoir *« effectué un calcul de logarithmes discrets dans une trappe des nombres premiers, en deux mois sur un cluster académique »*.

Traffic HTTPS et VPN déchiffrés

Les standards internationaux de cryptographie reposent sur des nombres premiers dont l'origine devrait être vérifiable. Mais, aujourd'hui, trop de serveurs communiquent en s'appuyant sur des nombres premiers dont l'origine est invérifiable : 37% des sites en HTTPS (parmi le million de sites les plus visités du top Alexa) et 13% des VPN IPsec, rappelle Inria.

Pour son propriétaire, une clé de chiffrement dotée d'une trappe ressemble à toute autre clé fiable. Pour les attaquants qui exploiteraient la trappe, en revanche, la sécurité de la clé peut être brisée à travers la résolution plus rapide du problème du logarithme discret. Selon les chercheurs, l'échelle de difficulté pour un pirate deviendrait *« très facile »* pour une clé de 768 bits, *« facile »* pour une clé de 1024 bits, mais hors de portée pour du 2048 bits…. pour le moment.

Chaque échange sécurisé par le standard Diffie-Hellman, qui utiliserait le nombre premier p, par exemple, pourrait être déchiffré par un attaquant ayant résolu le logarithme discret pour p. Des documents exfiltrés par Edward Snowden ont montré que la NSA américaine a utilisé cette approche.

Lire aussi :

Comment la NSA a (probablement) cassé le chiffrement par VPN

E. Thomé, Inria : « Les clefs de chiffrement de 768 bits ne suffisent plus »

L'informatique quantique, une épée de Damoclès pour le chiffrement