L’un des meilleurs algorithmes de chiffrement du monde vient de tomber

Ordinateurs (https://www.journaldugeek.com/category/ordinateurs/)

1 commentaire

Par **Tristan (https://www.journaldugeek.com/author/tristan/)** le 05 août 2022 à 12h30

Les algorithmes de chiffrement les plus puissants du monde ont parfois des failles toutes simples, il suffit de savoir les exploiter.

© TheDigitalWay / Pixabay

Il devait être l’algorithme de chiffrement parfait pour les années à venir. Tellement puissant que personne ne pourrait le briser, pas même avec des machines quantiques. Mais des chercheurs viennent de prouver que toutes ces annonces n’étaient que de la poudre aux yeux, et que nous avions encore beaucoup de travail à faire pour notre cybersécurité.

Tout commence le mois dernier quand le National Institute of Standards and Technology (NIST) annonce les grands gagnants de son concours de chiffrement. Lancé il y a des années, ce concours devait permettre d’accéder à une nouvelle méthode de chiffrement, bien plus développé que les solutions actuelles.

L’idée était même de réussir à se protéger contre ***l’hypothétique menace des ordinateurs quantiques (https://www.journaldugeek.com/2021/02/16/ordinateur-quantique-un-modele-de-bureau-commercialise-a-5000/)***. Si le NIST a retenu quatre grands vainqueurs, l’un d’eux a déjà les pieds dans le tapis. Baptisé SIKE, ce programme a été finaliste du concours du NIST, il fait donc partie des 8 derniers candidats retenus. Mais sa sécurité vient d’être remise en question, d’une façon, presque humiliante.

Une attaque menée par un ordinateur d’un autre âge

Une attaque vient de mettre à mal SICK, et non seulement cette nouvelle n’est vraiment pas une bonne publicité pour l’algorithme, mais c’est surtout la puissance de l’ordinateur assaillant qui inquiète. En effet, les chercheurs à l’origine de cette découverte on exploitait une brèche avec un ordinateur monocoeur, un appareil dont la puissance pourrait être comparée à celle de la dernière Apple Watch.

Ces appareils d’un autre temps sont censés être complètement largués technologiquement, mais voilà qu’ils ont réussi à faire tomber un système de chiffrement parmi les plus complexes au monde. Evidemment du côté de SICK, personne ne comprend encore vraiment bien ce qui vient d’arriver.

Pour David Jao, l’un des créateurs de l’algorithme « cette attaque était vraiment inattendue ». Pour les chercheurs qui ont mené l’attaque, cette nouvelle n’est pas des plus rassurantes. Originaires de Belgique, ils travaillent pour la plupart comme professeur à l’université de KU Leuven. Ils expliquent, dans leur article, que ***le processus de déchiffrement (https://www.journaldugeek.com/2017/06/21/parlement-europeen-chiffrement-protecteur/)*** a pris une petite heure.

La protection des données informatiques : une priorité absolue

Selon eux l’ordinateur aurait utilisé un protocole bien connu, qui a servi de socle à la création de SICK : le Supersingular Isogeny Diffie-Hellman ou SIDH. Si cette nouvelle est évidemment un très mauvais coup porté à l’ensemble du monde de la cybersécurité, cette annonce ne doit pas décrédibiliser la lutte pour la protection des données personnelles des utilisateurs.

Aujourd’hui le risque de piratage est plus grand que jamais, et les grandes nations de ce monde pourraient bien se livrer, dans les années qui viennent, une guerre numérique invisible. Alors pour éviter que notre modèle économique et tout ce qui est rattaché de près ou de loin à internet ne s’effondrent à la première attaque, il faut continuer de développer des solutions comme SICK. Elles auront toujours des failles, mais c’est justement en les découvrant que nous allons maximiser nos chances de nous protéger contre des attaques extérieures.

Vous pouvez retrouver le texte complet de l’étude belge ici. (https://eprint.iacr.org/2022/975.pdf)

Source: Gizmodo (https://gizmodo.com/quantum-encryption-algorithm-nist-broken-single-core-pc-1849360898)

chiffrement (https://www.journaldugeek.com/tag/chiffrement/)   **cyberattaque (https://www.journaldugeek.com/tag/cyberattaque/)**

(http…//www.journaldugeek.com/2022/08/05/malware voici-les-logiciels-les-plus-utilises-comme-chevaux-de-troie/)

1 Commentaire

Neccy
5 août 2022 at 14:13

SIKE ou SICK? Le nom change au court de l’article.

RÉPONDRE