Un gourou du chiffrement lance PrivaTegrity, une alternative à Tor

David Chaum est connu pour avoir été à l'origine de nombreux protocoles de chiffrement. C'est donc une voix qui compte. Il vient de travailler sur un concept de réseau de communication garantissant l'anonymat. Le nom de ce réseau est PrivaTegrity et le spécialiste a détaillé son invention lors de la conférence Real World Cryptography qui s'est déroulée à Stanford la semaine dernière.

L'objectif de ce travail est de corriger les erreurs de Tor, qui est actuellement le réseau d'anonymisation le plus connu et le plus utilisé. D'autres scientifiques se sont aussi attelés à cette tâche à travers les projets I2P, Hornet ou Vuvuzela. L'avantage de David Chaum est que Tor a été élaboré sur ses travaux passés, notamment le protocole d'anonymisation baptisé Mix Network. Ce dernier propose un chiffrement des données en couches en transitant par des serveurs intermédiaires. Il a été publié en 1979 et a servi de base pour le protocole Onion utilisé par Tor. A noter que ce protocole a également été repris par le ou les créateurs de Bitcoin.

Diviser, chiffrer et multiplier de manière aléatoire

Et c'est toujours sur ce protocole que David Chaum a travaillé pendant 2 ans, aidé par des laboratoires des universités américaines, anglaises et néerlandaises. Son article est intitulé « cMix: Anonymization by High-Performance Scalable Mixing ». Dans un schéma (cf ci-dessous), il explique que dans chaque chemin de communication établi dans un réseau cMix et de donner un exemple depuis un smartphone. Dans sa démonstration, le téléphone communique avec 9 serveurs de PrivaTegrity et l'application téléchargée génère une série de clés qu'elle partage avec chaque serveur. A chaque message envoyé, les données sont chiffrées en les multipliant avec cette série de clés. Ensuite les messages transitent dans chacun des 9 serveurs.

Ces derniers divisent le message avec sa clé et fractionne les données par un nombre aléatoire. Lors d'une seconde passe dans les serveurs, le message est intégré dans un lot de messages et chaque serveur modifie aléatoirement l'ordre du lot. *In fine*, les messages sont encore fractionnés avec un nombre aléatoire. Ce procédé est réversible pour permettre le déchiffrement des messages. Aujourd'hui, les équipes de Chaum élaborent une application de messagerie instantanée sécurisée s'appuyant sur PrivaTegrity.

Moins vulnérable que Tor

Selon David Chaum, en déplaçant la plupart des opérations de calcul du client vers le serveur, cMix atteint les mêmes vitesses de transfert que Tor. Mais contrairement à son homologue, cMix n'est pas vulnérable à différentes attaques dites de « tagging » qui visent à compromettre les nœuds Tor en traçant les points d'entrée des données et la localisation de leurs sorties. Le seul risque,

précisent les chercheurs, est d'arriver à compromettre l'ensemble des nœuds participant au chiffrement. Pour autant, ils revendiquent que « *PrivaTegrity fournit une confidentialité sur le plan technique qui n'est pas accessible à des Etats* ». Car selon eux, « *PrivaTegrity apporte une nouvelle approche pour l'identification des utilisateurs qui leur demande de fournir des bribes différentes d'informations d'identification à chaque mélange de nœuds* ». Cette identification peut prendre plusieurs formes, des mots de passe, des images, des numéros de téléphone ou des adresses mails.

Un anonymat géré par un conseil des sages

Si le chiffrement est réputé fort par les créateurs de PrivaTegrity, les chercheurs assurent que ce réseau n'est pas à 100% anonyme. Dans un entretien à *Wired*, David Chaum a expliqué que pour prévenir l'utilisation du réseau par des cybercriminels ou d'autres groupes illicites, il ensvisage la création d'un « *PrivaTegrity Council* ». Ce conseil donnerait accès aux données utilisateurs lors d'une requête de justice, mais seulement pour les personnes qui utilisent le réseau à des fins cybercriminels. Il serait composé de 9 membres au niveau mondial et doivent s'engager à transmettre les données demandées par les gouvernements. Cette proposition fait suite au débat intense aux Etats-Unis sur la demande des agences de renseignements d'installer des backdoors pour contourner le chiffrement des données. David Chaum et les chercheurs associés souhaitent que le contrôle se fasse par un conseil plutôt que par un Etat. Il reste maintenant à convaincre les internautes et les Etats de cette option.

A lire aussi :

Le chiffrement de Windows 10 sous écoute de la NSA ?

Payer Apple et Google pour le déchiffrement ?

crédit photo : nasirkhan / shutterstock