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

L'étude n'est pas nouvelle, nous l'avions d'ailleurs signalée dans nos colonnes en mai dernier. Mais elle vient d'être remise en lumière par une présentation effectuée par ses auteurs lors de la conférence ACM Computer and Communications Security. Sous un angle qui ne pouvait pas manquer de faire le buzz : les 14 chercheurs expliquent en effet avoir trouvé une piste expliquant comment les équipes de la NSA ont pu casser la plupart des algorithmes de chiffrement. Dans les documents exfiltrés par Edward Snowden, figure en effet une référence à une infrastructure de déchiffrement des communications VPN qu'aurait mise en place la célèbre agence de renseignement. Pour les spécialistes du chiffrement, cette mention pose évidemment la question du comment, les algorithmes de cryptographie étant précisément pensés pour générer toute une série d'échanges confidentiels et pour que chacun d'entre eux ne puisse être décodé qu'au prix de la mobilisation d'une puissance de calcul phénoménale. Difficilement compatible avec une infrastructure de déchiffrement 'à la volée' telle que la décrit le document dérobé par Edward Snowden. Même compte tenu des budgets pharaoniques de la NSA.

D'où l'importance des travaux des 14 chercheurs, dont des scientifiques issus de l'Inria et du CNRS (nous avions interviewé l'un d'eux, Emmanuel Thomé, dans nos colonnes en mai dernier). « *La clef du problème réside, de manière un peu ironique, dans l'échange de clefs Diffie-Hellman, un algorithme que nous et beaucoup d'autres ont défendu en le présentant comme un rempart contre la surveillance de mass*e, écrivent **Alex Halderman** et **Nadia Heninger**, deux des auteurs de l'étude. *Notre publication montre que, du fait de la rencontre de la théorie des nombres et de mauvais choix d'implémentation, de nombreux utilisateurs de Diffie-Hellman sont probablement exposés à des assaillants disposant des moyens d'un Etat.* » Diffie-Hellman est une méthode d'échanges de clefs qui fait partie des briques élémentaires de la cryptographie. Elle permet à deux personnes ne se connaissant pas de s'entendre sur un secret commun, et de communiquer dans des échanges à priori impossibles à déchiffrer par un tiers n'ayant pas ce secret en main. Cet algorithme est exploité dans l'initialisation de nombreux protocoles de sécurisation des communications : VPN, HTTPS, SMTPS…

Une machine Enigma des temps modernes ?

Concrètement, la faiblesse de Diffie-Hellman réside dans son implémentation, dans la « *transition entre les mathématiciens et les praticiens* », écrivent encore les deux chercheurs. En effet, pour amorcer un échange Diffie-Hellman, un serveur et un client doivent s'accorder sur un nombre premier (très grand), l'objet mathématique qui va rendre l'échange de clefs possible. Or, « *de nombreuses applications ont tendance à utiliser des primitifs (le nom technique donné à ces nombres premiers, NDLR) standardisés ou codés en dur* », reprennent Alex Halderman et Nadia Heninger. Et c'est là que réside la faille. Car, un attaquant peut, s'il en a les moyens, mobiliser d'importantes ressources pour précalculer ce primitif, « *puis déchiffrer aisément toute connexion individuelle utilisant ce primitif* ». « *En pratique, dans les systèmes de chiffrement déployés, ces primitifs sont peu nombreux* », expliquait en mai dernier dans nos colonnes Emmanuel Thomé, chargé de recherche à l'Inria Nancy, un des auteurs de l'étude.

Bien sûr, la tâche est simplifiée avec une faille de type LogJam, découverte par les mêmes chercheurs. Exploiter l'héritage technique d'une législation américaine limitant la taille de clefs – le principe de LogJam – facilite le précalcul du primitif. Mais, pour les chercheurs, même en dehors de cette attaque, la NSA a les moyens techniques de rendre Diffie-Hellman inopérant. « *Pour les implémentations les plus courantes de Diffie-Hellman (clefs de 1024 bits), cela coûterait une poignée de centaines de millions de dollars de construire une machine, basée sur du matériel spécifique, qui serait en mesure de casser un primitif Diffie-Hellman chaque année* », estiment Alex Halderman et Nadia Heninger.

Évidemment, l'effort paraît colossal, du niveau de celui produit par les Alliés pour décoder Enigma pendant la seconde guerre mondiale. Mais, pour les chercheurs, il serait payant : « C*asser un seul et très courant primitif de 1024 bits permettrait à la NSA de déchiffrer de façon passive les connexions de deux-tiers des serveurs VPN et d'un quart des serveurs SSH dans le monde. Casser un second primitif 1024 bits permettrait une écoute passive de 20 % des connexions d'un million des plus grands sites HTTPS de la planète.* » Bref, l'investissement initial ouvrirait la porte à l'écoute de milliers de milliards de communications que les utilisateurs pensent sécurisées.

Une simple hypothèse, mais qui colle aux faits

Pour les chercheurs, une telle décision est à la portée de la NSA. Le budget de l'agence de Fort Meade – de l'ordre de 10 milliards de dollars, selon un document Snowden – et les priorités de cette organisation (« *investir dans des capacités de déchiffrement révolutionnaires pour défaire la cryptographie adverse et exploiter le trafic Internet* », peut-on par exemple lire) sont compatibles avec cette hypothèse. Alex Halderman et Nadia Heninger expliquent n'avoir – pour des raisons évidentes – aucune preuve tangible du fait que la NSA exploite bien les faiblesses de Diffie-Hellman. Mais notent que leur hypothèse est compatible avec l'architecture du système de déchiffrement des communications VPN (Turmoil), décrite dans le document Snowden publié par Der Spiegel.

« *Les auteurs des travaux sur les faiblesses Diffie-Hellman ont très probablement raison quand ils affirment que la technique qu'ils décrivent est utilisée par la NSA, en masse, pour effectuer un déchiffrement à grande échelle du trafic Internet*, écrit Nicholas Weaver, un chercheur en sécurité de l'université de Berkeley en Californie, dans un billet de blog. *C'est peut-être la révélation technique la plus importante de ces dernières années sur les capacités de la NSA, dans la mesure où cela révèle le potentiel colossal de l'agence. Le protocole de réseau privé virtuel (VPN) IPsec, utilisé par des entreprises, des gouvernements et des particuliers partout dans le monde, est particulièrement vulnérable à cette faiblesse.* »

A lire aussi :

Emmanuel Thomé, Inria : « Les clefs de chiffrement de 768 bits ne suffisent plus »
SHA-1 : un algorithme clef du chiffrement HTTPS n'est plus sécurisé
Le chiffrement source de multiples failles de sécurité

Crédit photo : Maksim Kabakou / Shutterstock