Deux scientifiques comprennent enfin comment la NSA est parvenue à pirater des milliards de connexions cryptées

La NSA serait parvenue à décrypter des milliards de données à travers le monde grâce à l'échange de clés Diffie-Hellman.

Avec Franck DeCloquement
Avec Atlantico.fr

Le 6 juin 2013, Edward Snowden rendait public les détails des programmes de surveillance de masse américains et britanniques, parmi lesquels figuraient PRISM, XKeystore ou encore, Boundless Informant. Par l'intermédiaire du Washington Post, l'ancien informaticien à la CIA et à la National Security Agency (NSA), dévoilait des informations de la NSA classées top-secrètes, concernant la captation de métadonnées des appels téléphoniques aux Etats-Unis, ainsi que les programmes d'écoute et de surveillance à l'international. Au travers de ces révélations, le monde apprit alors qu'il n'avait aucun secret pour les autorités américaines et que chaque conversation téléphonique, chaque mail ou chaque SMS, pouvait être consulté, espionné et stocké dans les archives de la NSA, quelle que soit sa provenance ou sa destination.

Le journaliste Julian Assange révéla également que la NSA avait placé sur écoute plusieurs entreprises et cabinets français, marginalisant ainsi "l'économie industrielle", impactant le secteur de l'emploi et favorisant la hausse du chômage dans l'Hexagone. L'agence de renseignement aurait par ailleurs mis sur écoute des dirigeants politiques tels que Nicolas Sarkozy, Jacques Chirac, François Hollande et la chancelière allemande Angela Merkel. En révélant ces informations, Edward Snowden et Julian Assange brisèrent l'un des fondamentaux du renseignement américain : la discrétion.

Comment la NSA est-elle parvenue à décrypter des milliers de milliards de données ?

Mais comment la NSA est-elle parvenue à décrypter des milliards de données à travers le monde et à s'introduire dans notre intimité ? Comment l'agence de renseignement américaine arrive-t-elle à piloter les dessous des sociétés civiles ? Les informaticiens Alex Halderman et Nadia Heninger ont présenté leur théorie à la conférence ACM sur la sécurité informatique et des communications et évoqué, le piratage du décryptage des données, autrement dit l'utilisation de l'échange de clés Diffie Hellman. "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", ont-ils expliqué.

Selon eux, la NSA aurait exploité l'échange de clés Diffie Hellman, une méthode très complexe qui consiste à crypter et décrypter un échange par le biais d'un chiffre lambda. Ce moyen de communication permet à deux personnes (par défaut Alice et Bob) d'échanger sur un secret commun sans que personne ne puisse déchiffrer leur langage basé sur une combinaison mathématique. Il s'agit d'un algorithme exploité dans l'initialisation de nombreux protocoles de sécurisation des communications tels que VPN, HTTPS ou encore SSH.

Comment utiliser l'échange de clés Diffie Hellman ?

Selon Franck DeCloquement, "la méthode utilise la notion de groupe (multiplicatif), et un nombre premier. Dans ce cas, les opérations mathématiques - multiplication, puissance, division - sont utilisées telles quelles, mais le résultat doit être divisé par « p » pour ne garder que le reste, appelé modulo. Les groupes ayant la propriété de l'associativité, l'égalité $(g^b)^a = (g^a)^b$ est valide et les deux parties obtiennent bel et bien la même clé secrète".

L'utilisation de nombres premiers

Si la théorie d'Alex Halderman et de Nadia Heninger s'avérait exacte, la NSA serait parvenue à forcer le cryptage "considéré jusqu'à lors comme quasi incassable et utilisé très couramment sur les canaux de l'Internet non sécurisés (…) Elle serait donc en mesure de procéder à l'interception et au déchiffrement de milliers de milliards de connexions cryptées, et de mails privés", nous explique Franck DeCloquement. "Autrement dit, la NSA aurait trouvé le moyen pratique de casser ce chiffrement, qu'il faudrait en principe des centaines – voir des milliers d'années – en utilisant une méthode classique de décryptage, pour le résoudre. Inimaginable si cela était authentifié !"

La faiblesse de l'échange de clés Diffie Hellman réside dans son implémentation, dans la "transition entre les mathématiciens et les praticiens" ont indiqué les informaticiens. En outre, pour amorcer un échange Diffie-Hellman, un serveur et un client doivent se mettre d'accord sur un nombre premier qui deviendra l'objet mathématique capable de rendre l'échange de clés possible.

Quelles seraient les capacités de la NSA ?

Selon les informaticiens à l'origine de cette théorie, l'agence de renseignement n'aurait utilisé que quelques nombres premiers. Pour Franck DeCloquement, cela collerait parfaitement "avec les 11 milliards de dollars de budget annuel dédiés à l'Agence de Nationale de sécurité Américaine et dépensés pour révolutionner ses capacités de crypto-analyse".

"Casser un seul premier de 1024 bits (couramment utilisé dans l'échange de clés Diffie Hellman) 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", stipulent Alex Halderman et de Nadia Heninger. "Casser un second nombre premier 1024 bits permettrait une écoute passive de 20 % des connexions d'un million des plus grands sites HTTPS de la planète". En d'autres termes, "un investissement ponctuel dans le calcul massif permettraient d'écouter les milliers de milliards de connexions cryptées", précise Francke DeCloquement.

Sur son blog, Nicholas Weaver, chercheur en sécurité de l'université de Berkeley en Californie a estimé que la thèse des deux scientifiques était parfaitement plausible : "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".