

Les puces ne garantissent pas la sécurité des échanges en ligne

Article paru dans l'édition du Monde du 19.11.06

Un chercheur a trouvé un moyen, difficile à parer, de « casser » des clés de cryptage

La confiance qu'ont les utilisateurs d'Internet dans la capacité du système à sécuriser les données a toujours été relative. Elle pourrait bien s'effondrer si l'industrie des microprocesseurs et les fournisseurs de logiciels de cryptage se révélaient incapables de répondre à un nouveau type d'attaque, redoutablement efficace, découvert par une équipe conduite par le cryptologue allemand Jean-Pierre Seifert (universités d'Haïfa et d'Innsbruck). Le commerce en ligne serait alors menacé, mais aussi, plus largement, tout ce qui permet la dématérialisation des échanges, fondée sur des applications faisant appel aux codes secrets dits asymétriques, qu'il s'agisse de crypter, de signer ou de garantir l'intégrité de données numériques.

Dans un article encore confidentiel, le chercheur et ses collègues décrivent la façon dont ils ont pu, en une seule tentative - soit quelques millisecondes -, récupérer la quasi-intégralité d'une clé de cryptage de 512 bits (suite d'autant de 0 ou de 1). A titre de comparaison, la plus grande clé publique cassée à ce jour faisait 640 bits, et sa décomposition, annoncée en novembre 2005, avait mobilisé, pendant trois mois, 80 microprocesseurs cadencés à 2,2 GHz.

Depuis l'annonce, cet été, sur le serveur de l'Association internationale de recherche cryptologique (IACR), de la faisabilité théorique d'une telle attaque, les producteurs de microprocesseurs sont sur les dents : les puces de la quasi-totalité du parc informatique sont en effet vulnérables. Au point que le chef de la sécurité d'Intel, numéro un mondial des microprocesseurs, sollicité sur la question, fait répondre qu'il sera « indisponible pendant plusieurs semaines ». C'est que la parade face aux attaques classiques des systèmes à clé publique - à savoir allonger la taille des clés - est dans ce cas inopérante.

Jean-Pierre Seifert a en effet pris ces systèmes à rebours. Alors que leur robustesse s'appuie sur la grande difficulté à déduire mathématiquement la clé privée, secrète, à partir de son complément public, il s'est intéressé à la façon dont le microprocesseur lisait en interne ces données confidentielles.

Or il se trouve que le mode de fonctionnement même de la puce, optimisé pour accélérer les calculs, la rend vulnérable. « La sécurité a été sacrifiée au bénéfice de la performance », estime le chercheur.

On peut résumer ainsi le principe de l'attaque : pour aller toujours plus vite, le processeur fonctionne en parallèle et dispose d'un système de prédiction du résultat de l'opération en cours. Si la prédiction est bonne, le processus est sensiblement accéléré. Si elle est erronée, il faut revenir en arrière et recommencer l'opération élémentaire. Il « suffit » de mesurer le temps de calcul lorsque le processeur égrène la chaîne de 0 et de 1 qui constitue la clé de cryptage pour en déduire celle-ci.

Cette menace, qui porte le nom d'« analyse de prédiction de branche » (BPA), était déjà connue, mais elle nécessitait de très nombreux essais pour déduire de façon statistique la clé de cryptage. Ce qui la rendait impraticable. La percée de Jean-Pierre Seifert tient à ce qu'une seule écoute est désormais nécessaire. Et sa force réside dans le fait que le processus de prédiction, fondamental pour accélérer les performances du processeur, n'est pas protégé.

Un petit logiciel « taupe » pourrait donc écouter la puce en toute discrétion, et renvoyer la clé à des hackers, à des services de renseignement ou à des espions à la solde de concurrents.

« UNE QUESTION DE SEMAINES »

On n'en est pas tout à fait là. « Nous n'avons pas développé d'application clé en main, qui serait disponible en ligne », se défend Jean-Pierre Seifert. Mais il estime qu'une fois sa méthode dévoilée, début 2007, lors de la prochaine conférence RSA - du nom du système de cryptage le plus populaire -, la réalisation de tels logiciels d'attaque ne sera qu'« une question de semaines ».

Les spécialistes de cryptographie confirment le sérieux de la menace. Sous couvert d'anonymat, l'un des meilleurs connaisseurs mondiaux des systèmes à clé publique résume sans fard la situation : « La solution réelle est de revoir la conception même de nos microprocesseurs - un processus très long et difficile. Une solution de court terme serait de ne pas permettre que des applications sensibles tournent en parallèle avec des opérations standards sur un même ordinateur, ce qui est plus facile à dire qu'à faire dans un environnement de travail classique. Il reste des remèdes partiels, mais ils impliquent de ralentir considérablement le PC. »

Jean-Jacques Quisquater (Université catholique de Louvain, Belgique) rappelle que les normes militaires américaines mettent en garde depuis longtemps contre les attaques fondées sur l'analyse des temps de calcul. Pour lui, l'avenir est aux processeurs spécialisés dans les fonctions de sécurité. « Mais on n'y viendra pas avant plusieurs années », remarque-t-il.

« INTEL DOIT ÊTRE DÉSESPÉRÉ »

« On sait bien que ne sont très sûres" que les opérations cryptologiques conduites dans une enceinte protégée, côté serveur, avec un module spécifique », confirme Jacques Stern, directeur du laboratoire d'informatique de l'Ecole normale supérieure, à Paris. Une prophylaxie radicale, impraticable pour l'internaute lambda.

David Naccache (université Paris-II) reconnaît qu' « il n'y a pas d'opération à coeur ouvert possible » : toucher au système de module de prédiction pourrait affecter des fonctions essentielles.

En première ligne, Intel se borne à préciser de façon laconique que la prochaine version d'OpenSSL, un logiciel libre de sécurisation de données, répondra à la menace, au besoin en désactivant le module de prédiction. « Une telle mesure ralentirait par quatre le microprocesseur, assure Jean-Pierre Seifert, ce qui prouve à quel point Intel doit être désespéré. » Lui-même ancien collaborateur d'Intel et de son concurrent Infineon, revenu ensuite à l'université, il cherche désormais des parades à la faille qu'il a découverte. Mais dans la mesure où les recherches dans ce domaine sont récentes, prévient-il, « cela prendra un certain temps avant d'y voir clair ».

Certes l'assaut qu'il a conçu est plus difficile à mettre en oeuvre que les innombrables stratagèmes imaginés par les hackers, qui contraignent l'industrie à produire des « patchs » en permanence. Dans son cas, une simple rustine ne saurait suffire.

Hervé Morin