INVENTEURS DU MONDE NUMÉRIQUE

Communiqué de presse

Inria découvre une nouvelle faille dans le protocole TLS, garant de la sécurité des échanges sur Internet

Le 6 mars 2014, à l'occasion de la conférence IETF 89, une équipe de chercheurs Inria a annoncé la découverte d'une faille de sécurité importante du protocole TLS, le principal mécanisme de sécurisation des communications sur Internet. Cette faiblesse permettrait à un hacker, dans certaines circonstances, d'usurper l'identité des utilisateurs, en particulier sur les réseaux bancaires et d'entreprise. Cette faille concerne peu d'Internautes et un correctif est déjà disponible, mais les chercheurs d'Inria recommandent une révision en profondeur de TLS.

TLS, garant de la sécurité du web

Le protocole TLS est utilisé par tous les systèmes connectés : nos navigateurs, nos logiciels d'email, nos mobiles, nos box WiFi. C'est également le principal mécanisme de sécurité pour les échanges d'argent sur Internet. La fiabilité de ce protocole est hautement surveillée, en particulier depuis le scandale des écoutes de la NSA et les récentes failles critiques dans les produits Apple. Dans le cadre du centre de recherche commun Microsoft Research-Inria des chercheurs de l'équipe PROSECCO, du centre de recherche Inria Paris – Rocquencourt en collaboration avec leurs collègues de Microsoft Research ont voulu donner la preuve mathématique de la sûreté de TLS. Grâce à cette faille, un hacker déterminé pourrait usurper le certificat de sécurité d'un internaute via un serveur malicieux, par exemple pour effectuer un virement bancaire.

Le correctif déjà déployé

Seule une petite partie des adresses Internet en HTTPS sont concernées, uniquement lorsque le site demande un certificat ». Ces certificats sont nécessaires, par exemple, pour prouver son identité à une banque, ou se connecter au réseau interne de son entreprise. Les internautes concernés peuvent se mettre à l'abri facilement, en téléchargeant la dernière version du navigateur Chrome, Firefox, Internet Explorer ou Safari, d'ores et déjà protégés. La réactivité des éditeurs ne doit rien au hasard. L'équipe PROSECCO les a prévenu six mois à l'avance. *« Nous sommes habitués à travailler avec eux, témoigne Karthik Bhargavan*, chef de l'équipe PROSECCO. *Nous leurs avons proposé des solutions, et la plupart ont été adoptées. »*

D'autres failles à craindre

Mais pour Karthik Bhargavan, tous les problèmes de sécurité de ce protocole ne sont pas résolus. *« Nous avons ouvert une voie. D'autres informaticiens moins bien intentionnés risquent de s'y engouffrer. Si nous souhaitons éviter d'autres alertes semblables dans les prochaines années, il faut réviser le protocole TLS en profondeur. »* Dès cette semaine, l'équipe PROSECCO va entamer des discussions avec l'Internet Engineering Task Force (IETF), qui gère l'évolution du protocole TLS.

Pour en savoir plus :

Le site de l'équipe PROSECCO : http://prosecco.inria.fr
Le lien du projet : http://secure-resumption.com/

À propos d'Inria - www.inria.fr
Créé en 1967, Inria est le seul institut public de recherche entièrement dédié aux sciences du numérique. A l'interface des sciences informatiques et des mathématiques, les 3400 chercheurs d'Inria inventent les technologies numériques de demain. Issus des plus grandes universités internationales, ils croisent, avec créativité, recherche fondamentale et recherche appliquée. Ils se consacrent à des problèmes concrets, collaborent avec les acteurs de la recherche publique et privée en France et à l'étranger, et transfèrent le fruit de leurs travaux vers les entreprises innovantes. Les chercheurs des équipes Inria publient environ 5000 articles chaque année. Ils sont à l'origine de plus de 110 start-ups. Le budget primitif d'Inria s'élevait en 2013 à 233 millions d'euros dont 27 % de ressources propres.
Suivre Inria sur twitter.com/inria

Contact presse Inria - Muriel Droin – muriel.droin@inria.fr - 01 39 63 57 29

Contacts presse Thomas Marko & Associés –
Mathilde Folliot – mathilde.f@tmarkoagency.com - 01 44 90 87 42 – 06 20 39 05 48
Constance Nisio – constance.n@tmarkoagency.com – 01 44 90 87 40