CNRS : AmÃ©liorer la sÃ©curitÃ© des Ã©changes sur Internet
Internet
PostÃ© par : JPilo
PubliÃ©e le : 16/3/2009 15:00:00

Le protocole TLS est aujourd'hui le principal protocole utilisÃ© pour sÃ©curiser les Ã©changes sur Internet. Depuis quelques annÃ©es, il a subi des attaques qui ont entraÃ®nÃ© des usurpations d'identitÃ© et des falsifications d'informations. Pour y remÃ©dier, ***Mohamad Badra, chercheur CNRS au LIMOS , en collaboration avec la sociÃ©tÃ© Ineovation, a dÃ©veloppÃ© deux nouvelles extensions au protocole TLS***.
Ces normes viennent d'Ãªtre publiÃ©es par l'Internet Engineering Task Force, groupe international qui Ã©labore les standards InternetÂ : elles sont Ã la disposition des programmeurs et des Ã©diteurs de logiciel, qui peuvent maintenant les intÃ©grer dans les systÃ¨mes informatiques.

Le protocole de sÃ©curitÃ© SSL/TLS dÃ©veloppÃ© en 1995 par Netscape est aujourd'hui le principal protocole utilisÃ© dans le monde pour la sÃ©curisation des Ã©changes et des transactions sur Internet (commerce Ã©lectronique, comptes bancaires, enchÃ¨res en ligne, vote Ã©lectroniqueâ¦).

A cause de problÃ¨mes liÃ©s aux algorithmes cryptographiques utilisÃ©s par TLS, ce protocole prÃ©sente plusieurs inconvÃ©nients majeurs, notamment l'attaque Â« par collision Â», qui met Ã©galement en cause l'authentification Ã©tablie par des certificats numÃ©riques.

En collaboration avec la sociÃ©tÃ© Ineovation, Mohamad Badra, chercheur CNRS au laboratoire d'information, de modÃ©lisation et d'optimisation des systÃ¨mes Ã Clermont-Ferrand, a mis au point deux nouvelles extensions au protocole TLS afin d'amÃ©liorer sa sÃ©curitÃ©.

La premiÃ¨re extension concerne la mÃ©thode d'Ã©change de clÃ©s. Une clÃ© est un paramÃ¨tre nÃ©cessaire pour le chiffrement et le dÃ©chiffrement des donnÃ©es. Elle est soit symÃ©trique, soit asymÃ©trique. Dans le cas d'une clÃ© symÃ©trique, c'est la mÃªme clÃ© qui sert Ã la fois au chiffrement et au dÃ©chiffrement.

Pour la sÃ©curitÃ© des Ã©changes, elle doit rester secrÃ¨te et Ãªtre Ã©changÃ©e au prÃ©alable par l'Ã©metteur et le destinataire via un canal sÃ©curisÃ©. Dans le cas de clÃ©s asymÃ©triques, on utilise une clÃ© dite publique (connue de tous) pour le chiffrement de donnÃ©es Ã envoyer au destinataire, dÃ©tenteur de la clÃ© privÃ©e (secrÃ¨te).

Cette deuxiÃ¨me clÃ© est utilisÃ©e pour dÃ©chiffrer les donnÃ©es. L'avantage est de ne pas avoir besoin d'un canal sÃ©curisÃ© prÃ©Ã©tabli pour Ã©changer la clÃ©. L'extension dÃ©veloppÃ©e par Mohamad Badra utilise une nouvelle mÃ©thode d'Ã©change de clÃ©, basÃ©e sur une

association entre un algorithme asymÃ©trique et une clÃ© symÃ©trique.

On gÃ©nÃ¨re ainsi une clÃ© Â« fraÃ®che Â» au dÃ©marrage de chaque session, authentifiÃ©e par la clÃ© symÃ©trique. Cette nouvelle mÃ©thode est plus fiable, sÃ»re et plus performante que la mÃ©thode actuelle et elle simplifie le dÃ©ploiement de TLS dans les Ã©quipements rÃ©seaux, notamment sans fil et des fournisseurs d'accÃ¨s (par rapport Ã l'emploi de clÃ©s asymÃ©triques plus lourd Ã mettre en Å□uvre).

La seconde extension concerne la fonction de hachage des donnÃ©es. Cette fonction transforme le message en condensÃ¢t, c'est-Ã -dire en une suite de caractÃ¨res assez courte reprÃ©sentant le message. La moindre modification du message doit entraÃ®ner une modification du condensÃ¢t.

De plus, il est trÃ¨s difficile de retrouver le message original Ã partir du condensÃ¢t. Les fonctions de hachage) sont notamment utilisÃ©es pour garantir l'intÃ©gritÃ© des donnÃ©es (fonctions HMAC et pour la signature numÃ©rique. Dans le premier cas, lorsque le destinataire reÃ§oit le message, il calcule sa valeur HMAC et vÃ©rifie que c'est la mÃªme que celle qui a Ã©tÃ© envoyÃ© par l'Ã©metteur.

Dans le second cas, l'Ã©metteur souhaitant envoyer un message signÃ© doit calculer le condensÃ¢t du message et ensuite signer (chiffrer) ce condensÃ¢t avec sa clÃ© privÃ©e. Le destinataire utilise la clÃ© publique de l'Ã©metteur pour dÃ©chiffrer le condensÃ¢t et vÃ©rifie que c'est le mÃªme que celui qu'il a calculÃ© lui-mÃªme.

Depuis 2005, les fonctions de hachage les plus couramment utilisÃ©es (notamment MD5) ont fait l'objet d'attaques Â« par collision Â», c'est-Ã -dire que deux messages diffÃ©rents pouvaient donner des condensÃ¢ts identiques, ce qui remet en cause l'authentification par signature numÃ©rique avec le protocole TLS.

La seconde extension dÃ©veloppÃ©e par Mohamad Badra utilise de nouvelles fonctions de hachage assurant une meilleure protection contre les attaques par collision.