GITI

CRYPTOGRAPHIE ET STANDARDISATION

Comparée à d'autres disciplines scientifiques, la cryptographie présente la particularité de se développer en grande partie dans le domaine académique. Néanmoins, certaines de ses avancées ont des conséquences brutales dans le monde industriel. Un bel exemple de ce phénomène est l'effort actuel « SHA-3 » que le NIST (National Institute of Standards and Technology), l'organisme américain de standardisation, a initié en novembre 2007 et qui prendra fin en 2012.

Afin de bien comprendre les enjeux de cet effort de standardisation, il est nécessaire de brièvement s'intéresser à un objet très utilisé en cryptographie, à savoir les fonctions de hachage. En deux mots, une fonction de hachage est un algorithme cryptographique capable de calculer efficacement une empreinte de taille fixe (typiquement 160 ou 256 bits) à partir de n'importe quelle donnée de taille arbitraire. En pratique, les fonctions de hachage interviennent virtuellement dans toutes les applications sécurisées actuelles, comme le Web sécurisé, l'accès à notre courrier électronique ou au réseau de notre entreprise via un VPN, etc.

En août 2004, Xiaoyun Wang, Prof. de cryptographie dans une université chinoise, a démontré que la fonction de hachage SHA-1 (Secure Hash Algorithm), standard américain et de facto mondial, ne remplissait en fait pas son cahier des charges en termes de sécurité; en bref, Wang a « cassé » SHA-1, ainsi que presque toutes les autres fonctions de hachage que l'on connaît aujourd'hui, étant donné qu'elles partagent des caractéristiques identiques.

L'attaque contre SHA-1 reste certes difficile à mettre en pratique, mais elle était suffisamment sérieuse pour motiver le NIST à développer une nouvelle fonction de hachage. Pour trouver un successeur à SHA-1, le NIST a organisé l'effort de standardisation SHA-3 sous le modèle d'une compétition ouverte à toute personne et tout organisme dans le monde, ce modèle ayant démontré son succès il y a environ 10 ans pour développer l'AES (Advanced Encryption Standard). Le NIST a reçu 56 candidats, conçus aussi bien par des cryptologues amateurs, des cryptologues travaillant dans l'industrie ou venant du monde académique (un candidat, BLAKE, conçu par des chercheurs de l'EPFL et de la FHNW, représente la Suisse). À ce jour, 5 candidats ont été rejetés par le NIST avant la première ronde d'évaluation, et seuls 14 candidats ont été acceptés pour la deuxième ronde ; une troisième ronde réunira certainement les 4 ou 5 meilleurs. La fonction gagnante sera annoncée en 2012 et ses designers, à défaut de gagner de l'argent, auront le plaisir de voir le fruit de leur travail déployé dans une myriade d'applications.

On constatera que cet effort de standardisation fonctionne de manière complètement différente de ce que certains ont l'habitude de vivre dans le monde industriel. Mais, étant donné que notre environnement actuel ne peut plus se passer d'une fonction de hachage sûre, l'absence de retour économique n'a pas empêché des entreprises telles que France Telecom, Sony, Hitachi ou IBM de se lancer dans cette aventure.

Pascal Junod
professeur à l'HEIG-VD,
Yverdon-les-Bains
pascal.junod@heig-vd.ch