ASSEMBLÉE NATIONALE

12ème législature

Internet

Question écrite n° 60658

Texte de la question

Le monde de la cryptologie, cette science du chiffrement et du déchiffrement, est en pleine ébullition : une brique fondamentale des systèmes de signature électronique, qui permettent d'authentifier les messages, notamment sur Internet, semble en voie d'effritement accéléré. Une équipe chinoise vient en effet d'annoncer avoir sensiblement réduit la durée des calculs permettant de court-circuiter la fonction de hachage employée dans la plupart des systèmes de signature électronique. Cette information, si elle se confirmait, serait plus qu'inquiétante pour la sécurité de la transmission des données via Internet et ses réseaux sécurisés satellites. En conséquence, Mme Chantal Robin-Rodrigo demande à M. le ministre délégué à l'industrie de lui faire le point sur ce dossier, et de lui indiquer ses intentions à son sujet.

Texte de la réponse

Des avancées en termes de recherche ont en effet abouti à des attaques pour l'instant théoriques sur les fonctions de hachage. Ces avancées ne remettent pas en cause l'utilisation des applications de signature électronique dans l'immédiat, mais il convient de rester vigilant. À ce propos, la direction centrale de la sécurité des systèmes d'information (DCSSI) tient à disposition des industriels et des administrations un référentiel mis à jour régulièrement permettant d'adapter les caractéristiques des produits fournis ou utilisés aux exigences de sécurité requises en tenant compte des avancées technologiques. La migration progressive des systèmes de signatures électroniques vers de nouvelles techniques de chiffrement devrait donc permettre le maintien de la sécurité des signatures électroniques. À cette fin, il demeure essentiel d'accompagner la recherche française et européenne dans ce domaine. La DCSSI et certaines universités françaises sont très actives sur le sujet. Un travail de collaboration entre industrie et recherche - essentiel dès lors que des travaux de recherche fondamentale affectent directement des produits mis sur le marché -, est activement engagé au sein des réseaux d'innovation technologiques et des programmes européens de recherche dans le domaine de la cryptographie, et notamment dans le domaine des fonctions de. hachage. Le programme Oppidum du ministère chargé de l'industrie, plus orienté vers les applications et les usages, complète ce travail. Tous ces efforts seront prochainement à nouveau redoublés avec la création des pôles de compétitivité initiée par le Gouvernement et au sein desquels les projets d'innovation et de recherche dans le domaine de la sécurité des systèmes d'information pourraient mobiliser une part importante des actions.

Données clés

Auteur : Mme Chantal Robin-Rodrigo
Circonscription : Hautes-Pyrénées (2e circonscription) - Socialiste
Type de question : Question écrite
Numéro de la question : 60658
Rubrique : Télécommunications
Ministère interrogé : industrie
Ministère attributaire : industrie

Version web : https://www.assemblee-nationale.fr/dyn/12/questions/QANR5L12QE60658

Date(s) clée(s)

Question publiée le : 22 mars 2005, page 2896
Réponse publiée le : 19 juillet 2005, page 7162