Un proyecto busca mejorar la seguridad de la identificación y la autentificación en internet

Ua iniciativa de la Universidad de Salamanca quiere mejorar la seguridad en la identificación electrónica de los usuarios de internet, así como la autentificación de la información que envían. El objetivo del proyeto es contribuir a que las comunicaciones sean más seguras. Para ello, los investigadores trabajan en la modificación de los protocolos y los algoritmos de intercambio de información que se emplean en la actualidad y tratan de implementar otros nuevos.

DiCYT 2/3/2012 11:14 CEST

La Universidad de Salamanca trabaja en la modificación de protocolos y de algoritmos de intercambio de información.

Usos como la banca y el comercio electrónico o distintos servicios de las administraciones públicas requieren contar con una identidad electrónica. Aunque la seguridad es cada vez mayor también se están incrementando los

ataques que buscan conseguir suplantar identidades y acceder a información privilegiada. Por eso, Araceli Queiruga, del departamento de Matemática Aplicada de la Universidad de Salamanca, trabaja en esta línea. El año pasado año esta investigadora desarrolló un sistema de multifirma que permite que varias personas puedan firmar digitalmente un mismo documento. El resultado se plasmó en un programa diseñado en lenguaje Java.

En declaraciones a DiCYT, Queiruga explica las claves del nuevo trabajo. "Para usar un servicio electrónico tienes que identificarte y, cuando envías algo a alguien, esa persona tiene que estar segura de que eres tú quien envía la información y de que esa información es la que tú envías, que nadie la modifica en medio", comenta, distinguiendo así entre identificar a los usuarios y autentificar la información.

Cada sistema de criptografía se basa en diferentes problemas matemáticos. El RSA es un algoritmo basado en la factorización de números enteros y su funcionamiento depende de dos números primos secretos. Se trata del sistema más común, pero estos números son muy largos para aumentar la seguridad y esto complica las operaciones en dispositivos con poca capacidad. Por eso también se utilizan los logaritmos discretos basados en ecuaciones, aunque el problema es parecido. Finalmente, están los sistemas basados en curvas elípticas que tienen como principal virtud longitudes de la clave mucho menores con el mismo nivel de seguridad que los anteriores y, precisamente, en este campo es en el que indagará el proyecto.

El Instituto de Física Aplicada de Madrid, perteneciente al Consejo Superior de Investigaciones Científicas (CSIC), trabaja también en esta línea y colabora con Araceli Queiruga para avanzar de forma conjunta. "Es un trabajo lento, porque hay que averiguar qué es lo que ya está hecho y tratar de avanzar", comenta la investigadora.

Por otra parte, además de buscar nuevos protocolos y proponer nuevos algoritmos para mejorar la seguridad, una de las tareas de este proyecto es analizar los recientes métodos de ataque contra los algoritmos criptográficos. De esta manera los investigadores podrán conocer a qué se enfrentan.

Muchos tipos de firma

Entre las firmas digitales que se tratan de mejorar hay varias modalidades. Las firmas basadas en identidades hacen posible que un par de usuarios de un sistema pueda comunicarse información cifrada sin intercambiar claves. Las firmas delegadas o por poderes hacen que un firmante original pueda delegar su capacidad de firma digital en otra persona. Por otra parte, la firma ciega se emplea cuando el autor del mensaje y la entidad que lo firma son distintos para preservar la privacidad del autor, lo que puede ocurrir, por ejemplo, en transacciones comerciales.

El resultado de este proyecto, que está financiado por la Fundación Samuel Solórzano, será un programa informático que ayudará a avanzar en el campo de la seguridad electrónica.

TAGS | SEGURIDAD EN INTERNET | ALGORITMOS | AUTENTIFICACIÓN | CRIPTOGRAFÍA | IDENTIFICACIÓN |