

Cifrar el correo de forma eficaz y sencilla.

Dr. Dan Boneh de la Universidad de Stanford y Dr. Matt Franklin de la Universidad de California, fundadores de la empresa Voltage Security, han anunciado una nueva forma de comunicación cifrada que simplifica enormemente los estándares actuales usados en la criptografía asimétrica, asegurando que mantiene su eficacia. El invento se llama IBE (Identity-Based Encryption).

Aunque de forma comercial y como producto propietario, IBE simplifica la complicada estructura que requiere la criptografía asimétrica de clave pública y privada. Para su uso, se prescindir de una clave pública propiamente dicha, y se sustituye por algún dato que identifique unívocamente al individuo, como puede ser la propia dirección de correo, el número de teléfono o la dirección IP.

Voltage Security considera que la infraestructura necesaria para mantener una comunicación basada en criptografía asimétrica (PKI, Public Key Infrastructure) es demasiado costosa y compleja, lo que impide que llegue al público en general. Con esta nueva fórmula, no se requiere que los que se comuniquen posean ningún tipo de conocimiento sobre criptografía, ni se preocupen por sus claves, todo ocurre de forma transparente para ellos. Para poder cifrar y descifrar los emails, el método se integra totalmente en el habitual cliente de correo. De esta manera se eliminan la necesidad de certificados, autoridades certificadoras, repositorios de claves públicas, etc.

Según Voltage, *este nuevo algoritmo eleva la criptografía pública a un nuevo nivel por primera vez en dos décadas* y proporciona un estudio de 17 páginas sobre cómo funciona su algoritmo, descargable previo registro.

La criptografía asimétrica o de clave pública fue introducida en 1976 por Diffie y Hellman. Este criptosistema está basado en las propiedades matemáticas de los números primos, que permiten que cada interlocutor tenga una pareja de claves propias complementarias, una pública y otra privada.

También pretenden extender este algoritmo para su uso en las comunicaciones instantáneas, voz sobre IP y servicios web. Habrá que esperar para conocer su verdadero éxito comercial y repercusión real en Internet.

Más información y referencias:

Email Encryption, Simplified:

<http://www.enterpriseitplanet.com/security/news/article.php/2232431>

Your identity is the key to user-friendly encryption:

http://www.out-law.com/php/page.php?page_id=youridentityisthe1057760116&area=news

Voltage Security:

<http://www.voltage.com/>

Sergio de los Santos

<http://www.forzis.com>

Fecha artículo: 2003-07-10 13:47:43 - url artículo: <http://www.internautas.org/html/164.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org