EL PAÍS

CRÓNICAS DEL INTANGIBLE ›

¿En qué se basa nuestra moderna sociedad digital?

Internet se fundamenta en un cifrado que genera una clave dividida en dos partes, una que solo conoce el emisor y la otra, el receptor

SANTIAGO ESCOBAR ROMÁN

3 MAY 2016 - 17:18 CEST

Participantes en uno de los eventos de Campus Party, en São Paulo (Brasil). / REUTERS

En esta sociedad de personas interconectadas digitalmente, no tenemos tiempo de admirar los distintos artilugios electrónicos que utilizamos, como un ordenador, un móvil o una *tablet*, pero disponemos aún de menos tiempo para deslumbrarnos por las invenciones teóricas en las que éstos se fundamentan. Este es el caso del protocolo criptográfico de comunicaciones conocido como Diffie-Hellman.

Whitfield Diffie, responsable hace años de la seguridad en la empresa Sun Microsystems, y Martin E. Hellman, profesor emérito de la Universidad de Stanford, en California, han recibido recientemente el premio Turing 2015, el equivalente al Nobel de informática. Su invención, desarrollada a mediados de los años setenta (¡hace ya cuarenta años!), fue un hito en mecanismos de comunicación electrónica entre dos interlocutores, la base de la sociedad digital actual. Déjenme explicárselo con una analogía cotidiana para que entiendan el valor de dicha invención.

Imagínense ustedes en una habitación con un amigo situado en el otro extremo. Si quisieran enviarle una fotografía digital de forma electrónica, lo más seguro es que usaran el correo electrónico o la mensajería electrónica, seguro que con el omnipresente e insidioso WhatsApp. En esos casos, estarían haciendo uso ustedes del protocolo criptográfico Diffie-Hellman. De hecho, WhastApp ha empezado recientemente a cifrar los mensajes y utiliza Diffie-Hellman.

Cuando se envía a un amigo una fotografía de forma

> ***electrónica se está haciendo uso del protocolo criptográfico Diffie-Hellman. De hecho, WhastApp lo usa ahora para cifrar los mensajes"***
> ”

En los años setenta había pocas formas de enviar una fotografía digital a nuestro amigo y lo más común hubiera sido tender un cable entre los dos interlocutores y enviar el fichero a través del cable. Esto es lo que se conoce como un canal inalterable de comunicaciones, ya que es imposible que un intruso consiga acceder a lo que se envía por ese cable sin que nos diésemos cuenta. Pero supongamos que no se puede tender un cable con facilidad. La alternativa más común sería enviarlo suponiendo un canal inseguro de comunicaciones, donde un intruso podría interceptarlo. Obviamente, ese canal inseguro es, hoy en día, Internet y las comunicaciones inalámbricas como *wifi* y *bluetooth*. El uso de un canal inseguro requiere algún mecanismo de cifrado de mensajes. Sin embargo, para que un mecanismo de cifrado sea efectivo en la práctica es necesario usar una clave, es decir, algún factor de arbitrariedad que nos asegure que el cifrado de un mensaje depende no solo del contenido del mensaje sino también de la clave. Aquí es donde surge la maravilla de Diffie-Hellman.

Imagínense de nuevo en la habitación con su amigo en el otro extremo, utilizando un mecanismo de cifrado y una clave para enviarse la fotografía. Solo usted y su amigo conocen la clave y, por lo tanto, ningún intruso puede observar el contenido de los mensajes cifrados. Pero, claro, para que solo ustedes conozcan la clave, ambos deberían haberla acordado con anterioridad. En los años setenta, Diffie y Hellman buscaban un mecanismo de cifrado que no requiriese verse personalmente. Este tipo de intercambio de claves se conoce hoy en día como cifrado con clave asimétrica y es la base de Internet, ya que es complicado acordar una clave entre dos interlocutores en lugares lejanos, o esa clave acordada puede ser averiguada por un intruso. Lo que ellos buscaban era dividir la clave en dos partes, una que solo usted conozca y otra que solo conozca su amigo, evitando que un intruso aprenda la clave o alguna de las dos mitades.

> ***Diffie y Hellman buscaban un cifrado que no requiriese verse personalmente. Hoy en día se conoce como cifrado con clave asimétrica y es la base de Internet"***
> ”

La solución que obtuvieron fue fijarse en las matemáticas y, en concreto, en una propiedad muy interesante de la exponenciación, la permutación de exponentes. Se sabe que un número *a*, elevado a otro número *b*, cuyo resultado se eleva a otro número *c*, es equivalente a permutar los exponentes *b* y *c*, escrito en notación matemática como $(a^b)^c=(a^c)^b$. Por ejemplo, $(2^3)^4=4096=(2^4)^3$¿Y cómo se usa esta propiedad para generar una clave? Volvamos a la analogía, por última vez.

Imagínense en la habitación con su amigo en el otro extremo y ustedes dos van a utilizar el mecanismo de cifrado de Diffie-Hellman para enviarse la fotografía. El único requisito es que su amigo y usted hayan prefijado el valor del número *a*. Usted genera

la primera mitad de la clave escogiendo un número *b* aleatorio y calculando el número a elevado al número *b*, que envía a su amigo. Ahora su amigo genera la segunda mitad de la clave escogiendo también un número *c* aleatorio y enviándole a usted el número a elevado al número *c*. Ahora, usted y su amigo tienen los trozos necesarios para generar la clave sin que ésta haya sido enviada. Es decir, si usted toma el dato recibido de su amigo y lo eleva al número *b* escogido, obtiene el mismo número que si su amigo toma el dato que usted le envió y lo eleva al número *c* que él escogió.

> ***Los algoritmos existentes para calcular una clave tardan mucho tiempo. Sin embargo, esto podría no ser cierto conforme las computadoras aumentan su capacidad de cómputo o con la computación cuántica"***
>
> ”

Déjenme concluir enfatizando algunas propiedades prácticas. Primero, usted nunca ha revelado su número *b* y su amigo nunca ha revelado el número *c*. Esto es muy útil en situaciones inseguras, como cuando intenta acceder a una red *wifi* desde la calle. Segundo, esos números han sido generados aleatoriamente, así que no hay necesidad de acordarlos con antelación. Esta propiedad es muy útil cuando usted intenta conectar con algún dispositivo que no conoce anteriormente, por ejemplo, al acceder a una tienda o un banco en Internet. Tercero, fijar de antemano un número *a* no supone ningún riesgo, incluso aunque sea conocido por un intruso, si ese número es un número primo muy alto, ya que es prácticamente imposible extraer el número *b* o el número *c* de una exponenciación aunque se conozca el número *a*. De hecho, esta última propiedad es la base de nuestra sociedad digital y se apoya en la idea de que los algoritmos existentes para calcular el logaritmo, la función inversa de la exponenciación, tardan mucho tiempo. Sin embargo, esto podría no ser cierto conforme las computadoras aumentan su capacidad de cómputo o en el nuevo área de computación cuántica, por lo que existe mucha inquietud sobre si nuestra sociedad interconectada y segura puede peligrar en el futuro, pero ya hablaremos de esto dentro de otros 40 años.

Santiago Escobar Román es profesor titular de la Universitat Politècnica de València. Área Lenguajes y Sistemas Informáticos.

ARCHIVADO EN:

Alan Turing · Internet · Telecomunicaciones · Comunicaciones

Y ADEMÁS...