



DKIM: quizás no todo esté perdido frente al spam

Antes de las pasadas vacaciones pudimos leer una refrescante noticia en la que se nos decía que podríamos estar frente a un importante avance en la guerra contra el correo no deseado o "correo basura". Los actores principales de esa noticia eran Cisco y Yahoo, que estaban trabajando juntos en desarrollar un sistema, con la intención de convertirse en estándar IETF¹, para eliminar la plaga del spam.

Como no podía ser de otro modo, la esencia de esta nueva propuesta consistía en añadir sistemas de autenticación al correo electrónico actual. El sistema propuesto se conoce por sus iniciales en inglés DKIM (*Domain Keys Identified Email*)² y esta iniciativa cuenta con el apoyo de empresas como IBM, Verisign y Microsoft, entre otras. Dentro del grupo de desarrollo también hay representantes de las compañías Sendmail Inc. y PGP Corp.

DKIM ha sido desarrollada por ambas compañías desde agosto del pasado año y combina tecnologías anteriores de ambas. Yahoo y Cisco tienen intención de liberar de licencias y *royalties* su sistema, e incluso dejarlo dentro de la comunidad de código abierto. Hace mucho tiempo que se ha dicho que, en el futuro, será absolutamente necesario recurrir a sistemas de autenticación o de firmas criptográficas de los mensajes de correo-e para combatir el spam y otras lacras actuales, y la iniciativa DKIM parece que intenta hacer presente ese futuro.

Criptografía asimétrica

Esta propuesta utiliza la criptografía de clave pública para firmar los mensajes de correo, de modo que sus receptores puedan identificar fehacientemente a los remitentes y distinguirlos de otros, meros abusadores del correo electrónico, y poder detectar los correos propios de

Aún siendo el spam un viejo problema al que todo el mundo parece resignado a padecer, de vez en cuando hay iniciativas que intentan combatirlo. Yahoo y Cisco, entre otros, se han reunido para hacer una propuesta que, por simple, quizás pueda funcionar razonablemente bien. Hay que echarle un vistazo.

estafas como el *phishing*. En esta especificación confluyen elementos de dos fuentes distintas, por una parte del sistema **DomainKeys**, desarrollado por Yahoo y ya puesto en marcha en sus servicios de correo desde el pasado mes de noviembre –y que también ha sido adoptado por su competidor, Google Inc., en su servicio Gmail–, y la otra componente, que es la tecnología de identificación de mensajes de correo mediante cabeceras de firma, que fue establecida por Cisco.

En general, deben ser bien recibidas y apoyadas estas iniciativas para dotar de un poco de autenticidad a los correos electrónicos, siempre y cuando el sistema sea abierto, públicamente analizable y, sobre todo, voluntario.

El sistema DomainKeys sigue dos pasos para firmar y enviar un correo electrónico:

1. Establecimiento del sistema: el dueño del dominio genera un par de claves pública y privada para la firma y verificación de todo el correo que salga de ese dominio (se permiten varios pares de claves). La clave pública se distribuye a todo el mundo a través de DNS, y la clave privada se instala en todos los servidores de correo de salida.

2. Firma de mensajes: cuando un usuario autorizado envía un correo electrónico dentro del dominio, el sistema automáticamente genera la firma digital de ese mensaje. Esta firma se añade como prefijo en las cabeceras del mensaje y luego se encamina hacia sus destinatarios.

En el otro extremo, la recepción del mensaje se hace en tres pasos:

1. Preparación: los sistemas receptores de correo extraen la firma y el remitente (del cam-

po From:) de las cabeceras del mensaje, y luego obtiene la clave pública del dominio emisor del DNS.

2. Verificar: la clave pública obtenida del DNS se utiliza para verificar la firma del mensaje de correo y poder estar seguros de que fue enviado por y con el permiso del remitente indicado.

3. Entrega: el sistema de correo del receptor aplica sus políticas locales dependiendo de cual haya sido el resultado de la verificación de la firma. Si la firma no se verifica, o está

ausente, el mensaje de correo puede ser borrado, marcado, puesto en cuarentena, etc.

Este esquema es la más sencilla interpretación, de entre todas las posibles, de la definición de un servicio de autenticación por firma digital con un criptosistema asimétrico, y eso puede acarrear ciertos inconvenientes. Si uno cree necesario utilizar sistemas con no repudio, la primera pregunta que uno se hace es **¿por qué no usar S/MIME directamente?** Pues bien, la respuesta que dan los promotores no es del todo clara, y dicen que DomainKeys pretende ser un complemento natural al S/MIME pero funcionando en los sistemas servidor-servidor.

Sin entrar en demasiados detalles, sí hay que decir que el sistema propuesto resulta excesivamente *naïve* en lo que a la distribución y autenticación de las claves públicas se refiere, así como a la revocación de éstas. El sistema propuesto no sigue las burocráticas jerarquías del S/MIME, y se aproxima filosóficamente al escenario

"*inter pares*" del PGP; sin embargo, tiene aún varios temas pendientes de resolver después de su primer año de vida.

Incluso así, tenemos que recordar que, aún sin poderlo considerar un sistema completo, a pesar de todo, hay compañías bien conocidas que utilizan necesariamente el correo electrónico con valor transaccional con sus clientes, tales como bancos, sistemas de comercio electrónico, etc., y para ellos sus usuarios, los beneficios que aportan este tipo de sistemas para verificar la autenticidad de lo que se recibe, es algo esencial. Cualquier sistema de autenticación suficientemente robusto les ayudaría, a estos usuarios, a evitar ataques de *phishing* y otros tipos de suplantaciones hoy habituales dentro del correo electrónico.

Lo que quizás ya no esté tan claro es que se les pueda presentar como solución definitiva al *spam*, como hizo en su momento Microsoft con su iniciativa "Sender ID" y que les ha dejado un tanto aislados por problemas de licencias. El del *spam* es un problema complejo con muchas facetas, que incluyen la propia definición, la soberanía, etc., por lo que no es probable que acabe con él nada sencillo y simple que no sea la propia muerte de su sistema huésped, el correo electrónico.

Por ello, y a pesar de ello, creo que, en general, deben ser bien recibidas y apoyadas este tipo de iniciativas para dotar de un poco de autenticidad a los correos electrónicos; claro está, siempre y cuando el sistema sea abierto y públicamente analizable y, sobre todo, voluntario. Lo que es bueno para hacer negocios o prestar servicios, puede no serlo para la vida privada. ■

JORGE DÁVILA MUÑOZ

Consultor independiente
Director

Laboratorio de Criptografía
**LSIIS – Facultad
de Informática – UPM**
jdavila@fi.upm.es

¹ www.ietf.org/internet-drafts/draft-delany-domainkeys-base-02.txt editado en marzo de 2005.

² <http://antispam.yahoo.com/domainkeys>