SPF: Sender Policy Framework

por Álvaro Marín – alvaro@rigel.deusto.es

Desde que Ray Tomlinson en 1971 desarrollara la idea, el correo electrónico o e-mail ha sido uno de los mayores éxitos de Internet junto con la World Wide Web.
El poder enviar un documento de una parte a otra del mundo en unos segundos junto con su facilidad de uso, ha hecho de este servicio uno de los más utilizados.
Pero estamos hablando de una implementación del protocolo que data ya de hace muchos años y que no ha sido muy revisada ni mejorada desde el punto de vista de la seguridad (tenemos por ejemplo otros casos, como la nueva IPv6 que añade mejoras y más funcionalidades a la actual Ipv4), lo cual está provocando que actualmente el correo electrónico esté bajo amenaza. El usuario final en muchas ocasiones no se da cuenta de ésto, pero existe actualmente una batalla contínua en los servidores de correo que por ahora se está ganando, aunque quizás pueda llegar a perderse.

El protocolo utilizado para el intercambio de correo electrónico en Internet es el SMTP (Simple Mail Transport Protocol). Es el "idioma" mediante el cuál se hablan y entienden los MTAs (Mail Transport Agent), es decir, los servidores de correo. Por ejemplo, si yo escribiese un e-mail desde mi programa de correo, como puede ser Mozilla Mail, al dar al botón de "Enviar Mensaje" se crearía una comunicación entre mi ordenador y el servidor de correo que hayamos configurado.
Ésta se establece en base al protocolo SMTP. El servidor de correo que tengamos, se conectaría al servidor de correo del dominio del destinatario del mensaje para entregarselo, también por SMTP. El MTA destinatario, cogería dicho e-mail y lo colocaría en el buzón del usuario al que va dirigido para que éste lo pudiese leer mediante otro protocolo, como POP3.

Hace años, cuando no existían casi amenazas para el correo, los servidores recogían el mensaje y lo depositaban directamente en el buzón del usuario. Ahora sin embargo, la cosa ha cambiado bastante. Nuevas amenazas, como los virus hacen que ya desde los servidores se

tenga que actuar contra ellas, evitando así dejar en manos del usuario la seguridad de su sistema.
Debido a ello, existe un aumento en el desarrollo de aplicaciones para integrarse con el software que meramente implementa el protocolo SMTP y conseguir así por ejemplo, tener un antivirus que libre a los usuarios de código malicioso en su e-mail antes de bajárselo a su PC o sistemas que detecten y eliminen el correo no deseado.

Spam

El término SPAM tiene origen en los E.E.U.U. En el año 1937, una empresa dedicada a la charcutería llamada Hormel Foods, lanzó una lata con jamón y especias llamada Spiced Ham. El producto se hizo bastante famoso y el ejército americano lo usó en la Segunda Guerra Mundial. La palabra "spam" fue usada en una película de los Monty Python refiriendose a ello y apartir de ahí, se extendió su uso y se aplicó a los correos electrónicos cuyo destinatario no desea recibirlos y que son enviados masivamente.

Actualmente el 80% de correos electrónicos que puede recibir un ISP (Internet Service Provider), son spam. El objetivo del spam suele ser dar publicidad a ciertos productos a través del envío masivo de e-mails a usuarios para darlo a concocer. Esto supone, como es lógico, un consumo tanto de ancho de banda como de capacidad de proceso en el propio servidor.

Existen ya bastantes técnicas de prevención de spam, como BlackLists basadas en DNS (listas negras o direcciones desde las cuales no permitiremos recibir correo), filtros bayesianos, filtrado de contenido...uno de los más famosos y efectivos en este campo es el SpamAssassin, que combina una técnica de búsqueda de patrones en los e-mails para ir sumándole puntos hasta llegar a una puntuación en la cuál sería considerado como spam y reglas bayesianas que son capaces de autoaprender a partir de correos que se le hayan "escapado" al filtro.

Los spammers suelen usar servidores de correo mal configurados u open-relays, para enviar el correo. Por defecto, los MTAs permiten solo el envío de e-mail a través de él, es decir, que se pueda usar dicho servidor para el envío a otros dominios, solamente a la red en la que se encuentran. Por ejemplo, el servidor mail.deusto.es solo deja enviar correo a otros dominios desde dentro de la Universidad (actualmente se ha implantado un mecanismo por el cuál, teniendo usuario y contraseña en dicho
servidor se pueda enviar desde cualquier parte indicando al programa cliente de correo que use SMTP AUTH o SASL).
Si lo permitiese a cualquiera, estaríamos ante un caso de open-relay y seguramente no tardaría más de una hora antes de que fuese usado por spammers para enviar SPAM a través de él.

SPF: Sender Policy Framework

SPF [1] es un nuevo protocolo que operará junto con SMTP y DNS y que tiene como

objetivo detectar el envío de correo electrónico desde direcciones falsificadas, esto es, que nadie pueda enviar e-mails desde una cuenta de correo de un dominio que no le pertenece.
El envío de correo electrónico, está muy ligado al servicio DNS ya que realiza continuas consultas, por ejemplo, cada vez que tiene que enviar un e-mail para saber cuál es el registro MX de un dominio, que indica cuál es la dirección del MTA que
gestiona el correo para dicho dominio y poder así entregárselo.
Lo que hace SPF es consultar un registro más aparte del MX. Se trata del registro TXT que muchas veces se obvia o que sirve para dar ciertos datos de un dominio. Es en dicho registro donde situaremos cierta información que le servirá a SPF para calificar un e-mail como falsificado o no.

Por tanto, el servicio SPF se divide por un lado en publicar una serie de datos en el registro TXT del DNS de nuestro dominio y por otro, tener el software de SPF integrado con el MTA para que pueda realizar las consultas. Ambos son independientes, es decir, se puede tener un registro TXT listo para ser usado por el SPF de otros MTAs y no estar ejecutando SPF en nuestro servidor.

Si tenemos instalado el servicio SPF para nuestro servidor de correos, cada vez que le llegue un e-mail, hará una consulta DNS preguntando por el valor del registro TXT del dominio originario. Si no se instala dicho servicio, no se hará dicha consulta y todo funcionará como hasta entonces.

SPF está diseñado para verifiar o validar el "envelope sender", es decir, la cabecera "Mail From" no la cabecera "From"(que está dentro de la sección de "data") del e-mail.
Lo vemos en un ejemplo de una sesión telnet para el envío de correo:

split@pruebas:~$ telnet mail.deusto.es 25
Trying 130.206.100.17...
Connected to rigel.deusto.es.
Escape character is '^]'.
220 mail2.deusto.es ESMTP
helo mail.deusto.es
250 mail.deusto.es
mail from: prueba@rigel.deusto.es
250 Ok
rcpt to: alvaro@rigel.deusto.es
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
From: estoesloquesaleenelFROM@dominio.com
To: estoesloquesaleenelTO@otrodominio.com

Hola,
esto es una prueba :)
.
250 Ok: queued as 9E9CA4BFC
quit
221 Bye
Connection closed by foreign host.

Cuando recibamos el e-mail en el cliente de correo dará la impresión como que viene de la dirección estoesloquesaleenelFROM@dominio.com ya que es la que aparecerá en el campo From y que el destinatario es estoesloquesaleenelTO@otrodominio.com, cuando en realidad, somo nosotros.
Si nos fijamos en las cabeceras, se demuestra lo que ha pasado:

Return-Path: <prueba@rigel.deusto.es>
Delivered-To: 1almarin@rigel.deusto.es
Received: from localhost (unknown [127.0.0.1])
by mail1.deusto.es (Postfix) with ESMTP id AC1C724AFF9
for <1almarin@rigel.deusto.es>; Wed, 6 Oct 2004 10:02:39 +0200 (CEST)
Received: from mail1.deusto.es ([127.0.0.1])
by localhost (mail1.deusto.es [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id 13615-12 for <1almarin@rigel.deusto.es>;
Wed, 6 Oct 2004 10:02:24 +0200 (CEST)
Received: from mail (pruebas.deusto.es [130.206.100.132])
by mail1.deusto.es (Postfix) with SMTP id EF6FA24AFF4
for <alvaro@rigel.deusto.es>; Wed, 6 Oct 2004 10:02:09 +0200 (CEST)

El "envelope sender" o dirección origen real es *prueba@rigel.deusto.es* (no *estoesloquesaleenelFROM@dominio.com)* y la dirección destino real es *alvaro@rigel.deusto.es* (no *estoesloquesaleenelTO@otrodominio.com)* como se ve en la cabecera Received.

Es por ello, por lo que SPF se centra en la cabecera “Mail From”, que se corresponde con la cabecera Return-Path, en vez de en la cabecera From, que puede tener un valor cualquiera.

La información que deberemos añadir a nuestro registro TXT del DNS, puede constar de varios valores o una combinación de todos ellos. Los valores posibles son:

- v - versión del protocolo
- A – Registro A del DNS del dominio.
- MX – Registro MX del DNS del dominio.
- PTR – Registro PTR de la IP.
- IP4 – Direcciones IP de la v4.
- IP6 – Direcciones IP de la v6.
- EXISTS – Si el dominio indicado existe.

Imaginemos que recibimos un e-mail de una dirección de gnu.org (en su “Mail From”, recordemos) . Nuestro servidor de correo hará automáticamente algo como lo que hacemos a continuación:

$nslookup -type=txt gnu.org
Server: 130.206.100.1
Address: 130.206.100.1#53

Non-authoritative answer:
gnu.org text = "v=spf1 ip4:199.232.76.160/27 ip4:199.232.41.0/28 ?all"

es decir, preguntar por el contenido del registro TXT del dominio gnu.org, que es *"v=spf1 ip4:199.232.76.160/27 ip4:199.232.41.0/28 ?all"*.

Como se puede ver, el registro indica que las máquinas que pueden enviar legítimamente correo con dirección de origen @gnu.org (rms@gnu.org, por ejemplo), son las que están en el rango de IP(v4) 199.232.76.160/27 (199.232.76.160 - 199.232.76.191) y 199.232.41.0/28 (199.232.41.0 - 199.232.41.15).

El resto, en este caso, también serán legítimas ya que hay puesto un "?all"(neutral) al final de la regla, lo que la inutiliza (por si estamos en fase de pruebas o para ver los resultados sin descartar ningún correo). Si ponemos la etiqueta "-all"(fail) denegaríamos los demás orígenes y si ponemos "~all"(softfail) marcaríamos el correo con una cabecera llamada Received-SPF especial pero tampoco lo denegaríamos, sino que sería un filtro posterior adjunto al MTA, como maildrop, quien lo evaluaría.

Si hacemos una consulta de los registros MX de gnu.org, es decir, las máquinas que actuarán de servidores de correo para dicho dominio,

```
$nslookup -type=mx gnu.org
Server:         130.206.100.1
Address:        130.206.100.1#53

Non-authoritative answer:
gnu.org mail exchanger = 10 mx10.gnu.org.
gnu.org mail exchanger = 20 mx20.gnu.org.
gnu.org mail exchanger = 30 mx30.gnu.org.

Authoritative answers can be found from:
gnu.org nameserver = ns4.gnu.org.
gnu.org nameserver = ns1.gnu.org.
gnu.org nameserver = ns2.gnu.org.
gnu.org nameserver = ns3.gnu.org.
mx10.gnu.org    internet address = 199.232.76.166
mx20.gnu.org    internet address = 199.232.41.8
mx30.gnu.org    internet address = 199.232.41.6
ns4.gnu.org     internet address = 193.201.200.170
```

vemos que son mx10.gnu.org, mx20.gnu.org y mx30.gnu.org, y que sus correspondientes IPs 199.232.76.166, 199.232.41.8 y 199.232.41.6, entran dentro de dicho rango, ya que es lógico que desde sus servidores de correo sea desde donde se puedan enviar e-mails del dominio.

Vamos a ver otro ejemplo real de configuración de SPF. Tenemos el dominio blynx.com y su administrador solo quiere que las IPs de un determinado rango sean las legítimas para enviar correos con origen @blynx.com.

```
nslookup -type=txt blyx.com
Server:         130.206.100.1
Address:        130.206.100.1#53
```

Non-authoritative answer:
blyx.com text = "v=spf1 ip4:212.163.0.0/26 -all"

Si nosotros tuviesemos el servicio SPF en nuestro servidor de correo, al recibir un e-mail con la cabecera return-path con un valor @blynx.com, lo primero que haríamos sería consultar dicho registro. Una vez obtenido el valor del registro TXT comprobaríamos si la IP de origen de dicho e-mail pasa el test, es decir, que está dentro del rango indicado, 212.163.0.0/26.
En caso de que no estuviese, se rechazaría inmediatamente el e-mail, ya que tenemos un "-all".

Otro ejemplo, es el que utiliza el dominio linux.org:

nslookup -type=txt linux.org
Server: 130.206.100.1
Address: 130.206.100.1#53

Non-authoritative answer:
linux.org text = "v=spf1 a:ganymede.invlogic.com a:io.invlogic.com -all"

Si el servidor al que le llega un mail con mail from de @linux.org tiene el servicio SPF, consultará este registro y verá que solamente la IP correspondiente al registro A del dominio ganymede.invlogic.com y la IP del registro A de io.invlogic.com podrán enviar e-mail con dicho dominio por lo que los demás serán desacartados (-all).

Si quisieramos aplicar esto al dominio deusto.es, configurandolo de tal forma que los mails con la cabecera Return-path una dirección @deusto.es, solo puedan enviarse desde nuestro servidor de correo, mail.deusto.es, podríamos hacerlo añadiendo al registro TXT del DNS de la Universidad, la siguiente línea:

deusto.es. INT TXT "v=spf1 mx -all"

con lo que le estamos indicando en primer lugar, la versión de SPF que manejamos (spf1, versión 1), que la máquina que aparece como registro MX del dominio deusto.es es legítima para enviar correos con origen @deusto.es y que el resto no será permitido (-all).

Esta regla, puede parecer bastante restrictiva y de hecho lo es, ya que no legitimaría para nadie el envío de e-mail por ejemplo desde su casa con otro servidor de correo (como puede ser el del ISP contratado, terra, wanadoo, euskaltel...) con una dirección @deusto.es. Por ello, se recomienda la instalación de SASL ya que lógicamente no se puede dejar enviar a cualquiera correo a través del servidor, sino que en principio, solo a los clientes de nuestra red. SASL es la autentificación para el envío de correos a través del servidor, de tal modo que un usuario de la Universidad pueda enviar e-mails desde su casa a través del servidor de la Universidad, indicando su nombre de usuario y contraseña.

SPF tiene un problema con los e-mails reenviados, ya que el “evelope sender” se mantiene del emisario original. Para ello se han desarrollado una serie de parches[2] para la mayoría de MTAs, de tal modo que se evite dar como falsificado un e-mail que ha sido reenviado correctamente.

Como vemos, ésta es una técnica para verificar el origen de un e-mail, cosa que puede

ser interesante para la detección de spam, aunque no nos libraría de los open-relays.

Microsoft también estaba implementando una solución parecida llamada Caller ID [3], similar a SPF pero con XML que para este caso, no tiene mucho sentido debido a la limitación de espacio de los registros TXTs de los DNS. Según el RFC 1035, los paquetes UDP que deberán llevar la información de dicho registro, no deberían superar los 512bytes, por lo que el tamaño de éste, no debería ser mayor.
Lo que propone Microsoft es saltarse esta recomendación y hacer que la conexión se haga mediante TCP en vez de el UDP habitual usado para consultas DNS y poder llegar así a registros de hasta 2048bytes. Otra desventaja de Caller ID es que descarga por completo el mensaje antes de calificarlo como spam, mientras que SPF solamente lee las cabeceras.

El cofundador de PoBox Meng Weng Wong , creadora de SPF, se integró con Microsoft para plantear una solución común. Sender ID [4] ha sido el resultado y fue presentada para la estandarización a la Internet Engineering Task Force (IETF), pero ha habido numerosas posiciones en contra, como la de Apache Software Foundation [5] o Debian [6], rechazando esta tecnología debido a que su licencia sería incompatible con la idea de Open Source y contrario a los estándares abiertos de Internet. Finalmente, por el bien de Internet, la IETF ha rechazado Sender ID como estándar impidiendo así que una compañía con numerosos juicios por monopolio y con patentes sobre ideas o software sea la que controle el sistema de correo electrónico de Internet. Precisamente por este motivo, el de las patentes [7], ha sido rechazado SenderID.

[1] http://spf.pobox.com/

[2] http://spf.pobox.com/srs.html

[3]http://download.microsoft.com/download/2/e/2/2e2850b8-2747-4394-a5a9-d06b5b9b1a4c/callerid_email.pdf

[4] http://www.microsoft.com/mscorp/twc/privacy/spam_senderid.mspx

[5] http://www.apache.org/foundation/docs/sender-id-position.html

[6] http://www.debian.org/News/2004/20040904

[7] http://www.ietf.org/ietf/IPR/microsoft-ipr-draft-ietf-marid-core.txt

Alvaro Marín - alvaro@rigel.deusto.es