Bruno Sousa
<bruno/at/linuxfocus.org>

Introduzione a SPF

L'autore:

Bruno e' uno studente in Portogallo. Il suo tempo libero lo dedica a Linux ed alla fotografia

Premessa:

SPF sta per Sender Policy Framework e mira a costituire uno standard per prevenire la contraffazione degli indirizzi e–mail. Questo articolo fornisce una breve introduzione a SPF, i suoi vantaggi ed i suoi svantaggi.

Tradotto in Italiano da:
Roberto Pauletto
<neverquit/at/cwazy.co.uk>

SPF naque nel 2003, il suo mentore, Meng Weng Wong ha riunito le migliori caratteristiche di Reverse MX e DMP (Designated Mailer Protocol) per dare vita a SPF.

SPF usea il return–path (percorso di ritorno) (oppure MAIL FROM) presente nell'intestazinoe del messaggio email. Visto che tutti i MTA (Mail Transport Agent) lavorano con questi campi. Comunque Microsoft ha introdotto un nuovo concetto: il PRA (Purported Responsible Address – Indirizzo del supposto responsabile). Il PRA corrisponde all'indirizzo dell'utente finale che usa un MUA (come Thunderbird).

Quindi quando mettiamo insieme SPF ed il PRA possiamo ottenere l'identita' del mittente (il cosiddetto Sender ID). Quindi il Sender ID consente ad un utente che riceve email di eseguire il controllo del MAIL FROM – provenienza – (controllo SPF) ed il controllo PRA. In un qualche modo si puo' dire che i MTA verificheranno il MAIL FROM mentre i MUA eseguiranno il controllo PRA.

In effetti SPF necessita che DNS (Domain Name Sytstem) lavori propriamente. Questo significa che i record "reverse MX" devono essere diffusi, questi record dicono quale macchina *spedisce* l'email da un dato dominio. E' diverso dal record MX, usato oggigiorno, che spedifica la macchian che *riceve* email per un dato dominio

Che cosa serve a SPF per funzionare?

Per proteggere il vostro sistema con SPF dovete:

1. Configurare il vostro DNS per aggiungere il record TXT dove viene introdotta l'informazione che ceracata da SPF

2. Configurare il vostro sistema di email (qmail, sendmail) per usare SPF, cio' significa eseguire la verifica di ogni messaggio ricevuto sul vostro server.

Il primo passo verra' svolto sul server DNS dove si trova il dominio. Nella sezione successiva discuteremo circa i dettagli del record. Una cosa che dovete tenere presente e' la sintassi usata dal vostro server DNS (bind or djbdns). Ma non spaventatevi, il sito ufficiale di SPF fornisce un eccellente wizard (guida passo−passo) che vi spieghera' come fare.

Il Record TXT di SPF

Il record SPF e' contenuto in un record TXT ed il suo formato e' il seguente:

```
v=spf1 [[pre] type [ext] ] ... [mod]
```

Il significato di ciascun parametro e' il seguente:

<table>
<tr><th>Parametro</th><th>Descrizione</th></tr>
<tr><td>v=spf1</td><td>Versione di SPF. Usando SenderID dovreste vedere v=spf2</td></tr>
<tr><td>pre</td><td>Definisce un codice di ritorno quando esiste una corrispondenza.

I possibili valori sono:
Valore Descrizione
+ Default. Significa passato quando il test e' definitivo.
− Vuol dire test fallito. Questo valore in genere si applica a −all per dirgli che non si sono precedenti corrispondenze.
~ Vuol dire soft fail (fallimento non definitivo). Questo valore in genere viene applicato quando il test non e' definitivo.
? Vuol dire neutrale. Questo valore si applica di norma quando un test non e' definitivo.</td></tr>
<tr><td>type</td><td>Definisce il tipo da usare per la verifica.

Valori possibili sono::
Valore Descrizione
include per includere i test da un dominio fornito.
Scritto nella forma include:dominio
all to finire la sequenza dei test.
Ad esempio se e' −all, allora se tutti i test non sono stati completati fino a qui allora abbandona. Ma se non si e' sicuri puo' essere usato nella forma ?all che vuol dire il testo sara' accettato.
ip4 Usa una versione IP 4 per verifica.
Puo' essere usata nella forma ip4:ipv4 oppure ip4:ipv4/cidr per definire un raggio di valori. Questo e' il tipo maggiormente consigliato visto che mette il minor carico sui server DNS
ip6 Use una versione IP 6 for verifica.
a Usa un nome di dominio per verifica.
Eseguira' una ricerca nel DNS per una A RR .
Puo' essere usato nella forma a:dominio, a:dominio/cidr oppure a/cidr
mx</td></tr>
</table>

<table>
<tr><td></td><td>mx</td><td>Usa il DNS MX RR per verifica.
Il MX RR definisce il MTA ricevente, ad esempio se non e' lo stesso del MTA che invia, il test basato sul mx fallira.
Puo' essere usato nella forma mx:dominio, mx:dominio/cidr oppure mx/cidr.</td></tr>
<tr><td></td><td>ptr</td><td>Usa DNS PTR RR for verifica.
In questo caso viene usato un PTR RR ed una interrogaziore reverse map. Se l'host restituito e' compreso nelle stesso dominio la comunicazione e' verificata.
Puo' essere usato nella forma ptr:dominio</td></tr>
<tr><td></td><td>exist</td><td>Test per l'esistenza di un domninio .
Puo' essere scritto nella forma exist:dominio.</td></tr>
<tr><td>ext</td><td colspan="2">Definisce un'estensione opzionale per il tipo. Se viene omesso allora sara' usato solo un record di tipo singolo per l'interrogazione.</td></tr>
<tr><td>mod</td><td colspan="2">E' l'ultimo tipo di direttiva ed agisce come un modificatore di record.

modificatore Descrizione
redirect — Redirige la verifica verso l'uso dei record SPF del dominio definito. Usato nella forma redirect=dominio.
exp — Questo record deve essere l'ultimo e consente di personalizzare un messaggio di errore/avvertimento

<pre>IN TXT "v=spf1 mx -all exp=getlost.example.com"

getlost IN TXT "You are not authorized to send mail for the domain" (Non siete autorizzati ad inviare mail per il dominio)</pre></td></tr>
</table>

Hey, sono un ISP

Gli ISP (Internet Service Provider) avranno alcuni "problemi" con i loro utenti di roaming se non stanno usando meccanismi tipo POP−before−Relay invece che SASL SMTP.

Bene, se siete un ISP che si preoccupa dello spam e delle falsificazioni, dovreste riconsiderare le vostre regole di comportamento per quanto riguarda le email ed iniziare ad usare SPF
Ecco alcuni punti che potreste prendere in considerazione.

1. Per prima cosa configurate il vostro MTA per usare SASL, ad esempio potete abilitarlo sulle porte 25 e 587.
2. Avvisate i vostri utenti del fatto che state implementando delle regole. (spf.pobox.com vi fornisce un esempio, vedere i riferimenti).
3. Concedete ai vostri utenti un periodo di adattemento, nel senso che inserirete i vostri record di SPF nel DNS, me con i test softfail (−all) invece che con fail (−all).

Con questo avete protetto i vostri server, i vostri clients ed il mondo dallo Spam ....

Ci sono molte informazioni sul sito ufficiale di SPF per voi, cosa state aspettando?

Quali sono le cose da cui fare attenzione?

SPF e' una soluzione perfetta per proteggervi contro azioni fraudolente. Ha comunque un limite: il normale inoltro di e−mail (e−mail forwarding) non funzionera' piu'. Non potete semplicemente ricevere le e−mail nel vostro MTA e rispedirle. Dovete riscrivere l'indirizzo del mittente. Delle patch per i piu' comuni MTA si possono trovare in SPF side. In altre parole se iniziate ad inserire i record SPF DNS dovreste anche aggiornamre il vostro MTA per eseguire una riscrittura dell'indirizzo del mittente anche se non eseguite ancora la verifica dei record SPF.

Conclusione

Potreste pensare che l'implementazione verso SPF possa essere in qualche modo confusa. In realta' non e' complicato, inolte avete anche un gran wizard che vi aiuta a terminare il vostro compito (vedere la sezione riferimenti).

Se sete preoccupati per lo spam allora SPF vi aiutera', proteggendo il vostro dominio dalle contraffazioni, e tutto quello che dovete fare e' aggiungere una riga di testo nel vostro server DNS e configurare il vostro server email.

I vantaggi che SPF vi porta sono notevoli. In ogni caso, come ho gia' detto a qualcuno, non e' una differenza come dal giorno alla notte. I benefici di SPF si avranno col passare del tempo, quando anche altri vi aderiranno..

Ho parlato del Sender ID, e la sua relazione con SPF, ma non ho fornito alcuna spiegazione su di esso. Probabilmente la ragione la conoscete gia', la politica di Microsoft e' sempre la stessa, brevetti del software. Al riguardo di SenderID potete leggere la posizione di openspf.org .

In un prossimo articolo esamineremo la configurazione del MTA, arrivederci quindi.

Spero di avervi fornito una breve introduzione a SPF. Se volete saperne di piu', usate i riferimenti citati per scrivere questo articolo..

Riferimenti

Il sito ufficiale di SPF.
La FAQ ufficiale di SPF.
Il wizard ufficiale di SPF.
La posizione di openspf.org circa SenderID.
Un eccellente articolo circa SenderId e SPF.
Avverte i vostri utenti circa la conversione SASL
HOWTO − Definire un record SPF

Translation information:
en −−> −− : Bruno Sousa <bruno/at/linuxfocus.org>
en −−> it: Roberto Pauletto <neverquit/at/cwazy.co.uk>

2005−01−12, generated by lfparser_pdf version 2.51