RFC 7208 : Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 avril 2014

Date de publication du RFC : Avril 2014

https://www.bortzmeyer.org/7208.html

On le sait, le courrier électronique, tel qu'il est spécifié dans les RFC 5321 [1] et RFC 5322, ne fournit aucune authentification, même faible, de l'émetteur. Un expéditeur de courrier peut toujours prétendre être François Hollande <president@elysee.fr> et il n'y a aucun moyen de l'en empêcher. C'est parfois pratique mais c'est aussi un gros obstacle lorsqu'on tente de gérer le problème des courriers non désirés comme le spam. SPF vise à diminuer cette facilité de frauder en permettant à un titulaire de nom de domaine de déclarer quelle(s) adresse(s) IP sont autorisées à envoyer du courrier pour ce domaine. Ce nouveau RFC représente la première norme SPF (le premier RFC, le RFC 4408, était officiellement une expérimentation, sans le statut de norme.)

SPF dépend donc du DNS. Le principe de base est d'ajouter à sa zone DNS, par exemple bortzmeyer.org, un enregistrement de type TXT. Cet enregistrement déclare, dans un langage "*ad hoc*", quelle(s) adresse(s) IP peuvent envoyer du courrier pour ce domaine. Par exemple, bortzmeyer.fr a "v=spf1 mx -all", ce qui veut dire en français que seuls les MX (les serveurs qui reçoivent le courrier) de ce domaine peuvent en émettre, le reste de l'Internet (all) est exclu.

Pour voir ces enregistrements SPF, on peut par exemple utiliser dig :

```
% dig +short TXT bortzmeyer.org
"v=spf1 mx ?all"

% dig +short TXT freebsd.org
"v=spf1 ip4:8.8.178.116 ip6:2001:1900:2254:206a::19:2 ~all"

dig +short TXT archlinux.org
"v=spf1 ip4:66.211.214.128/28 ip4:78.46.78.247 ip6:2a01:4f8:120:34c2::2 a:aur.archlinux.org ~all"
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5321.txt

Le langage en question, très simple dans la plupart des cas (comme ci-dessus) mais permettant des choses très (trop ?) compliquées, est décrit dans la section 5 du RFC. Le premier enregistrement SPF contient `mx` indiquant que les machines dans l'enregistrement MX du domaine sont autorisées. Les deux autres enregistrements d'exemple listent explicitement les adresses IP. Notez qu'il existe plein d'exemples en annexe A de ce RFC.

Le langage de SPF, on l'a vu, est riche et complexe. D'où l'avertissement en section 11.1 de ce RFC : attention en l'évaluant. Il est prudent de prévoir des limites, par exemple de temps écoulé, du nombre d'inclusions emboîtées, ou de requêtes DNS envoyées, afin de ne pas être victime d'un déni de service (ou de contribuer à en faire un).

Et si on veut annoncer clairement qu'on n'envoie jamais de courrier ? Par exemple, un organisme de paiement a acheté des tas de noms de domaines dans plusieurs TLD mais il envoie toujours du courrier depuis `example.com` et l'usage de tout autre nom ne peut être qu'une erreur ou une tentative de fraude. On met alors un enregistrement `v=spf1 -all`. (Notez qu'il n'existait aucun mécanisme avant SPF pour annoncer qu'on n'envoyait pas de courrier. On voit parfois des MX bidons pour cela, par exemple pointant vers `0.0.0.0` mais cela n'est pas standard.)

On note que SPF, comme la plupart de ses concurrents, n'authentifie que le domaine, pas la personne émettrice (ce point, et plusieurs autres, est discuté en détail dans la section 11, « Sécurité », de notre RFC).

Le récepteur du courrier, s'il utilise SPF, va comparer l'adresse IP du client SMTP aux adresses autorisées par l'enregistrement SPF et le résultat pourra être (section 2.6) `none` (sans opinion, typiquement parce qu'il n'y avait pas d'enregistrement SPF publié), `neutral` (il y avait bien un enregistrement SPF mais il se terminait par un avis neutre, typiquement avec le qualificateur « ? », `pass` (cette adresse IP est autorisée pour ce domaine) ou `fail` (cette adresse IP n'est pas autorisée pour ce domaine). Il y a aussi deux cas d'erreurs, `temperror` et `pererror`.

Une fois que le domaine est authentifié, on en fait quoi ? En soi, être authentifié n'est évidemment pas une garantie de bon comportement (c'est toute la différence entre authentification et autorisation <https://www.bortzmeyer.org/authentifier-et-autoriser.html>). C'est simplement une première étape du processus de sécurité : une fois une identité solidement établie, on peut utiliser les mécanismes de réputation existants (en prime, un nom de domaine est plus stable qu'une adresse IP).

La décision finale est une décision locale. Les gens à qui on explique SPF pour la première fois disent souvent « et que fait le serveur SMTP si l'authentification SPF échoue ? » et la réponse est toujours « ça dépend », car, en effet, cela dépend de la politique de ce serveur SMTP. Certains seront violents, rejettant complètement le message, d'autres se contenteront de noter (peut-être en transmettant l'information avec le RFC 6652), d'autres enfin tiendront compte du résultat de SPF mais comme une indication parmi d'autres. Une fois la décision prise, le message peut être rejeté dès la session SMTP ou bien peut être accepté mais marqué d'une manière ou d'une autre (ce qui pourra lui « enlever des points » pour une évaluation ultérieure). Il existe deux façons de marquer un message, avec l'en-tête `Received-SPF:` (défini dans ce RFC, section 9.1) ou bien avec un en-tête non spécifique à SPF, `Authentication-Results:` (RFC 5451). Autre différence entre les deux en-têtes, `Received-SPF:` donne des informations détaillées, utiles pour le débogage, alors que `Authentication-Results:` vise surtout à donner un résultat simple sur la base duquel des logiciels ultérieurs (comme le MUA) pourront agir. Voici deux exemples, tirés du RFC :

```
Authentication-Results: myhost.example.org; spf=pass
     smtp.mailfrom=example.net

Received-SPF: pass (myhost.example.org: domain of
    myname@example.com designates 192.0.2.1 as permitted sender)
       receiver=mybox.example.org; client-ip=192.0.2.1;
       envelope-from="myname@example.com"; helo=foo.example.com;
```

Il y avait eu des discussions à l'IETF autour de la suppression d'un des deux en-têtes mais cela n'a finalement pas été fait.

Authentifier le courrier électronique est plus compliqué qu'il ne semble au premier abord, en partie parce qu'il existe plusieurs **identités** possibles :

— L'expéditeur de l'enveloppe (`MAIL FROM` de la session SMTP),
— L'expéditeur indiqué dans les en-têtes, qui lui-même dépend de l'en-tête qu'on choisit (`From:` ? `Sender:` ?).

Les partisans de la première approche (celle de SPF) lisent le RFC 5321 et s'appuient sur l'identité `MAIL FROM` (dite aussi `RFC5321.MailFrom`, cf. section 1.1.3). Chacune a ses avantages et ses inconvénients. (Notez que SPF utilise également le nom annoncé par la commande `HELO` de SMTP, cf. section 2.3.)

Attention, un vérificateur SPF doit bien prendre soin de n'utiliser que cette identité, autrement, les résultats peuvent être faux (par exemple, un MLM va changer le `MAIL FROM` mais pas l'en-tête `From:`).

Les changements depuis l'ancien RFC 4408 figurent dans l'annexe B. Le principal est le changement de statut : RFC 4408 était expérimental, notre nouveau RFC est sur le chemin des normes. Autrement, des détails, rien de vital, le principal changement technique étant l'abandon du type d'enregistrement DNS `SPF` pour les raisons expliquées dans l'annexe A du RFC 6686. Parmi les sujets polémiques qu'a rencontré le groupe de travail, et qui ont engendré l'essentiel du trafic sur la liste de diffusion :

— La décision douloureuse d'abandonner le type d'enregistrement DNS `SPF`.
— La revendication récurrente, par certaines personnes, que le RFC impose un traitement particulier (rejeter le message) en cas d'échec SPF. Comme cela n'affecte pas l'interopérabilité, le groupe a logiquement décidé que c'était une décision de politique locale.
— Il y a régulièrement une discussion dans le milieu SPF pour savoir ce que doit faire un serveur de messagerie lorsqu'il n'y a pas d'enregistrement SPF pour le serveur qu'il veut authentifier. Certains prônent un « enregistrement SPF par défaut » par exemple `v=spf1 all` ou encore `v=spf1 mx/24/48 a/24/48 all`. Une telle valeur est complètement arbitraire et n'a jamais été normalisée.
— Les discussions sur le "*forwarding*" de courrier et sur les listes de diffusion sont également des traditions du monde SPF.
— Pour des raisons de sécurité (nombreux traitements, et nombreuses requêtes DNS), certains avaient proposé d'abandonner la compatibilité avec les premières versions de SPF et de supprimer du langage quelques mécanismes très gourmands. Ce projet n'a pas été retenu.

SPF est aujourd'hui très répandu, de nombreux domaines l'annoncent et bien des logiciels de courrier peuvent traiter du SPF.