RFC 6652 : SPF Authentication Failure Reporting using the Abuse Report Format

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 juin 2012

Date de publication du RFC : Juin 2012

https://www.bortzmeyer.org/6652.html

Le but principal de ce RFC est d'améliorer l'utilisation du format ARF (RFC 5965[1]) pour rendre compte d'un problème d'authentification SPF. Ce protocole d'authentification du courrier électronique, normalisé dans le RFC 7208, n'avait pas de registre des modificateurs disponibles dans un enregistrement SPF. Ce RFC comble ce manque.

ARF est un format standard, structuré, permettant l'envoi de rapports d'incidents ou de problèmes (par exemple un spam) entre opérateurs. L'idée d'un format normalisé est de faciliter la production et la lecture automatique de ces rapports. Des extensions à ARF (RFC 6591 et RFC 6650) permettent de l'utiliser pour signaler des erreurs d'authentification.

SPF est un mécanisme d'authentification du courrier électronique qui fonctionne en listant les serveurs de courrier autorisés à émettre du courrier pour un domaine donné. Une fois l'émetteur connu, un récepteur peut alors appliquer ses politiques de sélection (accepter tous les messages en provenance de tel domaine, par exemple).

Les erreurs SPF peuvent être détectées par un récepteur de courrier, s'il fait des tests SPF, ou bien par un serveur de noms d'un domaine couvert par SPF : si on publie un enregistrement SPF spécialement fait pour cela (en utilisant les macros SPF qui permettent de récupérer plein d'informations sur la session SMTP en cours), le serveur DNS du domaine va voir passer les requêtes de vérification et pourra, par exemple, détecter une tentative d'usurpation pendant qu'elle se déroule.

Mais à qui signaler le problème ? Avant notre RFC 6652, il n'y avait pas d'autre moyen, en cas de problème SPF pour `example.net`, que d'écrire à `postmaster@example.net`. Désormais, la section 3 de notre RFC normalise des nouveaux modificateurs SPF, qu'on peut inclure dans ses enregistrements, et qui permettent d'indiquer des adresses de contact et les conditions sous lesquelles envoyer un beau rapport ARF conforme au RFC 6591 :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5965.txt`

— `ra=` ("*Reporting Address*") est le nom à utiliser à la place de `postmaster`. Si l'enregistrement SPF de `example.net` contient `ra=jimmy`, on enverra l'éventuel rapport à `jimmy@example.net` (il n'existe aucun mécanisme pour spécifier un autre nom de domaine comme `victim@somewhere.example`, afin d'éviter que le gérant de `example.net` puisse faire spammer d'autres domaines).
— `rp=` ("*Requested report Percentage*") est la proportion de problèmes SPF qui peut déclencher l'envoi d'un rapport. Si l'enregistrement SPF de `example.net` contient `rp=0`, il ne veut jamais être embêté par des rapports. Si l'enregistrement contient `rp=100`, il veut un rapport à chaque fois. Et s'il contient `rp=25`, il veut qu'un problème sur quatre, choisi au hasard, fasse l'objet d'un rapport. Cela permet de limiter le trafic répétitif. Notez qu'un champ du rapport ARF, `Incidents:` (section 3.2 du RFC 5965), permet d'indiquer que d'autres incidents sont connus mais ne font pas l'objet d'un rapport. Comme le note la section 6.2, à propos de la sécurité, le volume de rapports envoyés peut être conséquent (et pas connu à l'avance).
— `rr=` ("*Requested Reports*") permet d'indiquer par quelle sorte de rapport on est intéressés (`all` = tous, `f` = erreurs fatales, etc, voir section 4.1).

Ces modificateurs SPF sont enregistrés dans le tout nouveau registre IANA `<https://www.iana.org/assignments/spf-parameters/spf-parameters.xml>`, créé par ce RFC 6652 (section 5). Il inclut les modificateurs de la liste ci-dessus ainsi que `exp=` et `redirect=` qui avaient déjà été normalisés par le RFC 4408. Désormais, ce registre est ouvert à de futures additions, selon les règles « Norme nécessaire » du RFC 5226.

Tirés de l'annexe B, voici des exemples d'enregistrements SPF du domaine `example.org` utilisant les nouveautés de notre RFC. D'abord un cas simple, avec juste une demande que les rapports soient envoyés à `postmaster` :

```
v=spf1 ra=postmaster -all
```

Un cas un peu plus compliqué, toujours avec un seul modificateur :

```
v=spf1 mx:example.org ra=postmaster -all
```

Et un cas qui utilise tous les modificateurs de ce RFC. On demande que 10 % des rapports d'erreur (pas d'échec d'authentification, non, des erreurs lorsque l'enregistrement SPF ne peut être analysé, cf. RFC 7208, sections 2.6.6 et 2.6.7) soient envoyés à `postmaster` :

```
v=spf1 mx:example.org -all ra=postmaster rp=10 rr=e
```

Il reste à voir quel sera le déploiement de ce système. Apparemment, plusieurs fournisseurs de logiciels y travaillent.