RFC 6650 : Creation and Use of Email Feedback Reports: An Applicability Statement for the Abuse Reporting Format (ARF)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 juin 2012

Date de publication du RFC : Juin 2012

http://www.bortzmeyer.org/6650.html

Le format ARF, normalisé dans le RFC 5965 [1] permet à des acteurs de l'Internet (typiquemet des FAI et des gros hébergeurs de courrier comme Gmail) de s'envoyer des rapports structurés, produits et analysés automatiquement, au sujet des abus commis avec le courrier électronique, notamment du spam. Ce nouveau RFC du groupe de travail qui a conçu ARF expose comment et dans quelles circonstances utiliser ARF.

L'idée de base d'ARF était qu'un message serait détecté comme abusif (par exemple par l'utilisateur cliquant un bouton « C'est du spam ! ») et que cette détection déclencherait l'envoi d'un rapport ARF au responsable (qui pourra le faire suivre, si nécessaire). En comparaison avec un rapport non structuré, l'avantage d'ARF est que les messages ARF seront analysables par des programmes, pour rendre leur traitement plus efficace.

(Il existe des extensions à ARF pour des usages qui ne sont pas forcément des abus ou des erreurs d'authentification, comme l'extension du RFC 6430 mais elles sont encore peu déployées et pas étudiées ici.)

Ce RFC 6650 est largement inspiré d'un document externe à l'IETF, le RFC 6449. En quelque sorte, il en est la version officielle.

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

Les autres documents existants, comme la norme ARF (RFC 5965), sont purement techniques (définition d'un format) et ne répondent pas à des questions comme « à qui envoyer les rapports ? » ou « que faut-il mieux mettre dans un rapport ? », qui font l'objet de ce RFC.

D'abord, faut-il un accord explicite du destinataire avant d'envoyer les rapports ARF ? La section 3 considère qu'il y a deux cas, celui de deux acteurs décidant entre eux de se transmettre des rapports ARF, relatifs à leurs clients. C'est le cas le plus fréquent aujourd'hui. Et le second cas est celui où des rapports non sollicités sont envoyés à quelqu'un dont l'expéditeur pense qu'il est concerné. En l'absence d'un accord préalable, ces rapports ne feront pas forcément l'objet de la même attention.

La section 4 détaille le premier cas, les rapports attendus. En vrac, elle demande, entre autres :

— Que l'accord entre les deux acteurs soit respecté, notamment dans le choix de l'adresse de destination (`arf-feedback@example.net`, par exemple).
— Que le rapport soit à la syntaxe ARF (évidemment) et que les éléments optionnels dans ARF soient inclus, s'ils sont disponibles (pas de rétention délibérée). Cela concerne `Original-Mail-From`, `Arrival-Date`, `Source-IP`, `Original-Rcpt-To`.
— Pour relativiser la demande précédente, il peut y avoir occultation délibérée, pour préserver la vie privée, comme détaillé dans le RFC 6590.
— Enfin, la section 4 demande (vœu pieux ?) que le récepteur **agisse** lorsqu'il reçoit des rapports qui le concernent (section 4.3 du RFC 6449).

La section 5 s'attaque aux rapports inattendus, envoyés sans concertation préalable. Elle est bien plus longue puisqu'il s'agit d'embêter des gens qui n'ont rien demandé (dans le précédent cas, les deux parties ont pu se mettre d'accord sur tous ces points, qui doivent être explicités ici.) Les auteurs du RFC demandent, entre autres :

— Que le destinataire ait un moyen de ralentir le rythme d'envoi des rapports, pour que son infrastructure ne s'écroule pas sous la charge (il n'existe pas de mécanisme standard pour cela, cela doit être fait « à la main »).
— Que l'expéditeur s'assure que ses messages soient crédibles, pour diminuer le risque qu'ils soient jetés sans autre forme de procès. Cela implique notamment une authentification SPF et/ou DKIM correcte.
— Que l'expéditeur soit bien conscient qu'un traitement effectif des rapports reçus a un coût pour le destinataire et qu'il fasse donc attention à produire des rapports techniquement corrects et factuellement sérieux.
— Que l'expéditeur n'envoie pas automatiquement des rapports sur la base d'une analyse automatique. Les logiciels de classification peuvent se tromper et prendre pour du spam ce qui n'en est pas. Il serait anormal de générer un spam (le rapport ARF) en échange d'un message qui n'en est pas un. (Je vois au boulot pas mal de rapports violant cette règle, réalisés en format ARF ou pas, qui sont manifestement automatiquement émis par un logiciel, et un logiciel particulièrement débile en plus.) La section 5 de notre RFC recommande d'utiliser plutôt les messages identifiés comme spam par un humain, ou bien ceux reçus par un pot de miel.
— Que le MUA, s'il fabrique des rapports ARF, les envoie au fournisseur de service de l'utilisateur, **pas** au supposé responsable du message abusif. Actuellement, il existe plusieurs logiciels qui automatisent partiellement l'envoi de messages de plainte et qui, pour trouver le destinataire, font des requêtes whois au petit bonheur la chance (par exemple pour tous les AS sur le chemin suivi), avant d'envoyer la plainte à dix ou quinze adresses dont la plupart ne sont en rien responsables du message abusif. La bonne pratique est donc d'envoyer à son fournisseur, charge à lui de faire suivre intelligemment. Pour cela, il devra compter sur diverses heuristiques mais, au moins, il sait les utiliser.
— Que le rapport soit correctement rempli, indication du bon `Feedback-TYpe:` (RFC 5965, section 3.1), indication de toutes les informations pertinentes, etc. Par contre, pas besoin d'hésiter avant de choisir le format ARF : les rapports qui suivent ce format sont lisibles manuellement, même si le destinataire n'a pas de logiciel adapté.

— Que le destinataire agisse, sur la base des rapports corrects. Il existe des tas de rapports incorrects (envoyés au mauvais destinataire, par exemple) et le format ARF permet d'automatiser une partie du triage. Par exemple, le FAI peut regarder l'en-tête `Source-IP:` du rapport et jeter sans autre forme de procès les rapports où ladite adresse IP source ne fait pas partie de ses préfixes IP. Malgré cela, il y a quand même des rapports corrects ce qui ne signifie pas qu'ils seront lus <http://www.bortzmeyer.org/abuse-ne-repond-pas.html>. Le RFC discute également de la délicate question de la réponse : faut-il signaler à l'envoyeur du rapport que son message a été lu et qu'on a agi ? (Actuellement, même si les rapports d'abus sont traités, l'utilisateur ne reçoit jamais de retour.) La conclusion est que ce serait souvent une bonne idée que de signaler à l'émetteur du rapport qu'il n'a pas travaillé pour rien.

Les recommandations précédentes concernaient surtout les rapports envoyés en réponse à un message abusif, du spam par exemple. La section 6 couvre les rapports signalant un problème d'authentification, avec SPF ou DKIM. Ces rapports utiliseront le `Feedback-Type: auth-failure` (RFC 6591) et sont normalisés dans des documents comme le RFC 6652 et le RFC 6651. Les demandes pour cette section sont :

— Qu'on n'envoie de tels rapports qu'à ceux qui les demandent, et aux adresses de courrier qu'ils ont indiqué,
— Qu'on n'envoie pas de rapport ARF pour un problème d'authentification d'un rapport ARF (pour éviter les boucles). C'est aussi pour éviter ces boucles que le rapport doit être envoyé avec un `MAIL FROM` vide (plus exactement ayant la valeur <>),
— Qu'on fasse attention aux attaques avec amplification. Il ne faut pas qu'un méchant fabrique un faux, juste pour que l'échec de l'authentification de ce faux déclenche l'émission d'un gros rapport ARF à destination d'un pauvre FAI qui n'y est pour rien.

Quelques pièges de sécurité peuvent attendre les utilisateurs du format ARF. La section 8 en fait le tour. D'abord et avant tout, les rapports ARF peuvent être des faux, fabriqués de A à Z (afin, par exemple, de faire accuser un innocent). La confiance qu'on leur accorde doit dépendre de l'authentification de l'émetteur et de la confiance qu'on accorde à cet émetteur. (C'est un problème ancien, voir par exemple la section 4.1 du RFC 3464.)

Le modèle originalement envisagé pour ARF était celui du rapport déclenché manuellement ; un utilisateur se plaint, il clique sur le bouton « Ceci est un spam », le message est transmis au fournisseur de messagerie qui fabrique un rapport ARF et l'envoie. Le rythme d'envoi des rapports restait donc limité. Au contraire, les évolutions récentes d'ARF, notamment pour le signalement de problèmes d'authentification, vont vers des rapports déclenchés automatiquement. Un message arrive, le test SPF échoue, paf, un rapport ARF est généré et envoyé. Cela peut mener à des rythmes d'envoi bien plus grands, qui peuvent dépasser les capacités de réception et de traitement du destinataire. C'est d'autant plus ennuyeux qu'un attaquant vicieux pourrait générer exprès des problèmes d'authentification, pour déclencher ces envois massifs. Il peut donc être raisonnable de limiter le débit d'envoi de tels rapports.

Autre façon de traiter ce problème : ne pas envoyer un rapport par incident. Le format ARF prévoit (RFC 5965, section 3.2) d'indiquer dans le rapport combien d'incidents similaires il couvre (champ `Incidents:`). On peut donc choisir, par exemple, de n'envoyer qu'un rapport pour N incidents ou, mieux de faire une décroissance exponentielle (un rapport par incident pour les 10 premiers, un rapport par série de 10 incidents pour les 100 suivants, etc).