RFC 5965 : An Extensible Format for Email Feedback Reports

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 31 août 2010. Dernière mise à jour le 1 septembre 2010

Date de publication du RFC : Août 2010

https://www.bortzmeyer.org/5965.html

Les opérateurs de réseaux et de serveurs, aujourd'hui, passent beaucoup de temps à s'envoyer des rapports indiquant qu'un message reçu est en fait abusif, spam ou hameçonnage. Ces rapports sont désormais bien trop nombreux pour être traités manuellement et il est donc nécessaire de définir un format standard pour les représenter, de façon à permettre un minimum de traitement automatique sur ces rapports. C'est ce que fait notre RFC, le premier du groupe de travail MARF <http://tools.ietf.org/wg/marf>. Ce format s'appuie évidemment sur MIME.

Avant l'adoption du format MARF (qui précède sa normalisation formelle dans ce RFC), plusieurs opérateurs avaient défini des formats privés (section 1). Cela rendait évidemment difficile l'analyse des rapports envoyés, il fallait écrire du code pour chaque opérateur. Désormais, il existe donc un format standard, basé sur le type MIME `multipart/report` normalisé dans le RFC 6522 [1]. Ce format utilise le sous-type (« type du rapport ») `feedback-report`.

Ce n'est pas la première tentative de normalisation dans ce domaine, les précédentes n'ont pas été des succès.

Ce RFC ne fait que normaliser un format, il ne spécifie pas à qui les rapports doivent être envoyés, comment les authentifier, ou ce qu'il faut en faire, il se focalise sur l'aspect technique. Le cahier des charges figure en section 1.2 :

— Le format devait être lisible à la fois par un humain et par un programme,
— Le message signalé devait être inclus dans le rapport,

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6522.txt`

— Le format devait permettre l'ajout de métadonnées,
— Le format devait être extensible.

Ces objectifs ont-il été atteints ? Voyons la définition du nouveau format (une certaine familiarité avec le RFC 5598 est utile).

La section 2 du RFC décrit le format MARF. Un message MARF est donc un message MIME `multipart/report`, tel que défini dans le RFC 3462. Le type du rapport est `feedback-report` (donc le message contiendra un en-tête du genre `Content-Type: multipart/report; report-type=feedback-report; ...`). Chaque rapport ne concerne qu'un seul message, il n'y a pas de mécanisme pour l'agrégation de messages. Il comprend trois parties MIME obligatoires :

— La première est une description en langue naturelle du rapport,
— La seconde est un ensemble de métadonnées structurées, de type MIME `message/feedback-report`,
— La troisième est le message original, de type `message/rfc822` en général (rappelez-vous que MIME est récursif et qu'il est donc parfaitement possible d'avoir un message MIME dans un autre message MIME).

Le sujet du rapport doit être le champ `Subject:` du message original, éventuellement avec un préfixe comme `FW:` (pour "*forwarded*"), ce qui me semble déroutant car, en examinant sa boîte aux lettres manuellement, on ne distingue pas facilement les spams des rapports sur les spams.

Focalisons-nous un instant sur la seconde partie, les métadonnées. Le format de ce nouveau type MIME `message/feedback-report` est décrit dans la section 3. Cette partie est composée de plusieurs champs, suivant la syntaxe des en-têtes du courrier (attention, seule leur syntaxe est identique, un champ de même nom qu'un champ du RFC 5322 n'a pas forcément la même sémantique). Comme pour tout le contenu du rapport, le destinataire ne doit pas forcément leur faire une confiance aveugle. Ils représentent des assertions du créateur du rapport et ne sont pas forcément vérifiables.

La liste des champs n'est pas fixée définitivement, de nouveaux champs pourront être enregistrés dans le futur. Aujourd'hui, la liste des champs obligatoires comprend (section 3.1) :

— `Feedback-Type:`, défini dans la section 3.5,
— `User-Agent:`, indiquant le logiciel qui a produit le rapport,
— `Version:`, aujourd'hui toujours 1.

Il y a aussi des champs facultatifs, parmi lesquels (sections 3.2 et 3.3) :

— `Arrival-Date:` indiquant l'heure de réception,
— `Authentication-Results:` qui indique les résultats des procédures d'authentification, tels que formalisés par le RFC 7001,
— `Incidents:`, un nombre indiquant le nombre de fois que ce message a été reçu,
— `Reported-Domain:`, qui indique le nom du coupable présumé (par exemple parce que le message vient de lui),
— `Reported-URI:`, qui indique un URI pertinent pour le rapport, par exemple l'URL d'un site Web de hameçonnage pour lequel un spam faisait de la publicité,
— `Source-IP:`, indiquant l'adresse IP source au moment où le message est entré dans le domaine qui génère le rapport,
— Et bien d'autres (la liste complète et à jour figure dans le registre `<https://www.iana.org/assignments/marf-parameters/marf-parameters.xhtml>`). Notez que certains champs facultatifs peuvent apparaitre plusieurs fois (comme `Reported-URI:`) et d'autres une et une seule fois (comme `Arrival-Date:`).

Un exemple d'une telle partie :

```
Feedback-Type: abuse
User-Agent: SomeGenerator/1.0
Version: 1
Arrival-Date: Thu, 8 Mar 2005 14:00:00 EDT
Source-IP: 192.0.2.1
Authentication-Results: mail.example.net;
              spf=fail smtp.mail=somespammer@example.com
Reported-Domain: example.com
Reported-Uri: http://example.com/earn_money_fast.html
```

La grammaire complète figure en section 3.5.

On le sait, le courrier électronique est une jungle où tout est possible. Les rapports peuvent être mensongers ou, tout simplement, incorrects techniquement. Que faire dans ce cas ? La section 4 est claire : de tels messages devraient être ignorés ou rejetés. Le principe de robustesse (« Acceptez n'importe quoi et essayez de le décoder ») ne s'applique pas aux questions de sécurité.

Je l'ai dit plus haut, une des exigences du cahier des charges était l'extensibilité. La section 6 expose les moyens déployés par MARF pour atteindre ce but. Notamment, deux registres IANA sont créés, pour pouvoir ajouter des nouvelles données : le registre des types de retours ("*feedback types*") et celui des champs dans les métadonnées. Les types et les champs inconnus doivent donc être ignorés par les programmes, afin de pouvoir ajouter des nouveaux sans casse.

Les registres en question sont décrits de manière plus formelle dans la section 7. Celle-ci décrit l'enregistrement du nouveau type MIME `<https://www.iana.org/assignments/media-types/message/> message/feedback-report`, le nouveau registre des métadonnées `<https://www.iana.org/assignments/marf-parameters/marf-parameters.xhtml>` (dans lequel on peut enregistrer par la procédure « spécification obligatoire » du RFC 5226) et le nouveau registre des types de retour `<https://www.iana.org/assignments/marf-parameters/marf-parameters.xhtml>` (même procédure pour l'enregistrement). Aujourd'hui, ce registre contient des types comme "*abuse*" (courrier non sollicité), "*fraud*" (courrier de tentative d'escroquerie), "*virus*" (courrier contenant un virus), etc.

Comme tout ce RFC porte sur un problème de sécurité, il est normal que la section dédiée à ce sujet, la 8, se demande si le nouveau format est lui-même sûr. Elle met notamment en garde contre les interprétations abusives (section 8.2) : cette norme décrit juste un format, elle ne garantit pas que les rapports, même syntaxiquement corrects, soient authentiques. Le mécanisme par lequel on décide de faire confiance (ou pas) à un rapport n'est pas spécifié par ce RFC. Il est donc déconseillé de déclencher automatiquement des actions (comme l'inscription sur une liste noire) sur la seule base d'un rapport, sans précautions supplémentaires.

Par exemple, le RFC recommande que les rapports soient un minimum authentifiés, par le biais de techniques comme SPF, DKIM ou S/MIME (ce dernier est conseillé mais, curieusement, PGP n'est pas cité).

Autre problème de sécurité lié à ces rapports, le risque d'attenter à la vie privée. La section 8.5 rappelle que la règle devrait être d'envoyer des rapports complets mais, si la protection de la vie privée le nécessite, qu'on peut supprimer certaines parties du rapport pour ne pas révéler d'informations privées. (Même si on devine que cette idée de vie privée défrise considérablement les auteurs du RFC.)

Peut-on générer automatiquement des rapports MARF (section 8.6), par exemple parce qu'un pot de miel a reçu un spam ? Le RFC met en garde : un attaquant qui sait qu'un tel générateur existe pourrait l'utiliser pour faire fabriquer des rapports contre ses ennemis, en envoyant de faux spams.

Encore un piège amusant : les rapports seront souvent générés pour des messages qui contiennent du logiciel malveillant. Ledit logiciel va se trouver dans la partie du rapport qui reprend le message original. Les processeurs de messages MARF doivent donc faire attention à ne pas, par exemple, exécuter accidentellement le méchant logiciel (section 8.7) !

Un exemple plus complet est cité dans l'annexe B2 du RFC (le message original a le sujet "*Earn money*" et prétend venir de `somespammer@example.net`) :

```
From: <abusedesk@example.com>
Date: Thu, 8 Mar 2005 17:40:36 EDT
Subject: FW: Earn money
To: <abuse@example.net>
MIME-Version: 1.0
Content-Type: multipart/report; report-type=feedback-report;
  boundary="part1_13d.2e68ed54_boundary"

--part1_13d.2e68ed54_boundary
Content-Type: text/plain; charset="US-ASCII"
Content-Transfer-Encoding: 7bit

This is an email abuse report for an email message received from IP
192.0.2.1 on Thu, 8 Mar 2005 14:00:00 EDT.  For more information
about this format please see http://www.mipassoc.org/arf/.

--part1_13d.2e68ed54_boundary
Content-Type: message/feedback-report

Feedback-Type: abuse
User-Agent: SomeGenerator/1.0
Version: 1
Original-Mail-From: <somespammer@example.net>
Original-Rcpt-To: <user@example.com>
Arrival-Date: Thu, 8 Mar 2005 14:00:00 EDT
Reporting-MTA: dns; mail.example.com
Source-IP: 192.0.2.1
Authentication-Results: mail.example.com;
            spf=fail smtp.mail=somespammer@example.com
Reported-Domain: example.net
Reported-Uri: http://example.net/earn_money.html
Reported-Uri: mailto:user@example.com
Removal-Recipient: user@example.com

--part1_13d.2e68ed54_boundary
Content-Type: message/rfc822
Content-Disposition: inline

From: <somespammer@example.net>
Received: from mailserver.example.net (mailserver.example.net
  [192.0.2.1]) by example.com with ESMTP id M63d4137594e46;
  Thu, 08 Mar 2005 14:00:00 -0400
To: <Undisclosed Recipients>
Subject: Earn money
MIME-Version: 1.0
Content-type: text/plain
Message-ID: 8787KJKJ3K4J3K4J3K4J3.mail@example.net
Date: Thu, 02 Sep 2004 12:31:03 -0500

Spam Spam Spam
Spam Spam Spam
Spam Spam Spam
Spam Spam Spam
--part1_13d.2e68ed54_boundary--
```

Qui utilise ou utilisera ce format ? Je n'ai pas trouvé sur le site officiel <http://www.mipassoc.org/arf/> de liste des implémentations (pour générer et analyser du MARF). Il faut se contenter des liens en <http://wordtothewise.com/resources/arfdeveloper.html>. Voir par exemple :

- <http://rubyforge.org/projects/arfparser/>
- <http://search.cpan.org/perldoc?Email::ARF>
- <http://abusix.com/solutions>

Mais, apparemment, plusieurs opérateurs utilisent déjà ce format. Idéalement, on devrait pouvoir l'utiliser pour soumettre des rapports à abuse@opérateur.net et à des organismes comme Signal-Spam

<https://www.bortzmeyer.org/signaler-a-signal-spam.html> (ce dernier semble tout à fait mort). Mais cela ne semble pas possible actuellement. En tout cas, au bureau, seule une minorité des rapports de spam que je reçois sont pour l'instant à ce format (je ne peux pas les reproduire ici, pour des raisons de protection des données personnelles ; dans beaucoup de cas, le rapport est erroné et je ne veux pas que des innocents se trouvent mentionnés). Un autre document, plus récent, le RFC 6650, décrit en détail dans quels cas utiliser ARF et comment.