RFC 6591 : Authentication Failure Reporting using the Abuse Report Format

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 avril 2012

Date de publication du RFC : Avril 2012

https://www.bortzmeyer.org/6591.html

Le format ARF, normalisé dans le RFC 5965 [1], permet d'envoyer des rapports **structurés** (analysables par un programme) à propos d'un message électronique abusif, spam ou hameçonnage, par exemple. Ce RFC 6591 spécifie une extension à ARF pour le cas où le problème avec le message est un échec d'un mécanisme d'authentification. On peut ainsi prévenir l'émetteur que quelqu'un essaie d'usurper son identité ou, plus fréquemment aujourd'hui, qu'il y a une erreur dans la configuration de ses mécanismes d'authentification.

Par exemple, si le message est authentifié par SPF (RFC 7208 et RFC 6652), il arrive assez souvent que l'émetteur se mette à utiliser un MTA non prévu et non listé dans l'enregistrement SPF. Si ce dernier se termine par un `-all`, l'usage de ce MTA va se traduire par une erreur d'authentification. L'extension ARF décrite ici permettra de transmettre un rapport à l'émetteur, pour qu'il corrige.

L'extension consiste en un nouveau type de rapport ARF, `auth-failure` (section 3.1), rejoignant les rapports existants <https://www.iana.org/assignments/marf-parameters/marf-parameters.xml#marf-parameters-2> (comme `abuse` ou `fraud`). Un rapport de ce type va comporter, dans sa seconde partie (celle qui est structurée, la première étant en langue naturelle et la troisième étant le message original), les champs suivants. À noter que certains étaient déjà définis par le RFC 5965 mais peuvent avoir des exigences différentes ici (par exemple, être obligatoires pour les rapports `auth-failure` alors qu'ils étaient optionnels pour les autres). Les nouveaux sont désormais dans le registre IANA <https://www.iana.org/assignments/marf-parameters/marf-parameters.xml#marf-parameters-1>. Commençons par les champs obligatoires :

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

— `Auth-failure:` Nouveauté de ce RFC, il indique en un mot la raison de l'échec. Les valeurs possibles sont `adsp` (cf. RFC 5617), `bodyhash` (le condensat cryptographique du corps du message ne correspond pas à la signature), `revoked` (signature DKIM expirée), `signature` (signature DKIM invalide, cf. RFC 6651), `spf` (échec SPF, RFC 6652).
— `Authentication-Results:` Normalisé dans le RFC 7001, il indique les paramètres d'authentification et les raisons de l'échec.
— `Reported-Domain:` Le nom de domaine annoncé par l'expéditeur.

D'autres champs sont recommandés ou simplement optionnels :

— `Original-Envelope-Id:` Un identifiant unique pour la transaction SMTP (cf. section 2.2.1 du RFC 3464)
— `Original-Mail-From:`
— `Source-IP:`
— `Delivery-Result:` Ce dernier indique la décision qui a été prise après l'échec de l'authentification (jeter le message, le distribuer quand même, etc)

Il peut en outre y avoir des champs spécifiques à certaines techniques d'authentification. Par exemple, pour DKIM (RFC 6376), les champs `DKIM-Domain:`, `DKIM-Identity:` et `DKIM-Selector:` ou pour SPF le champ `SPF-DNS:`..

Voici un exemple (annexe B du RFC) de rapport ARF sur un échec d'authentification DKIM, par suite d'une incohérence entre le contenu effectif et ce qu'indiquait la signature :

```
Message-ID: <433689.81121.example@mta.mail.receiver.example>
From: "SomeISP Antispam Feedback" <feedback@mail.receiver.example>
To: arf-failure@sender.example
Subject: FW: You have a new bill from your bank
Date: Sat, 8 Oct 2011 15:15:59 -0500 (CDT)
MIME-Version: 1.0
Content-Type: multipart/report;
  boundary="------------Boundary-00=_3BCR4Y7kX93yP9uUPRhg";
  report-type=feedback-report
Content-Transfer-Encoding: 7bit

--------------Boundary-00=_3BCR4Y7kX93yP9uUPRhg
Content-Type: text/plain; charset="us-ascii"
Content-Disposition: inline
Content-Transfer-Encoding: 7bit

This is an authentication failure report for an email message
received from a.sender.example on 8 Oct 2011 20:15:58 +0000 (GMT).
For more information about this format please see [this memo].

--------------Boundary-00=_3BCR4Y7kX93yP9uUPRhg
Content-Type: message/feedback-report
Content-Transfer-Encoding: 7bit

Feedback-Type: auth-failure
User-Agent: Someisp!Mail-Feedback/1.0
Version: 1
Original-Mail-From: anexample.reply@a.sender.example
Original-Envelope-Id: o3F52gxO029144
Authentication-Results: mta1011.mail.tp2.receiver.example;
 dkim=fail (bodyhash) header.d=sender.example
Auth-Failure: bodyhash
DKIM-Canonicalized-Body: VGhpcyBpcyBhIG1lc3NhZ2UgYm9keSB0
  aGF0IGdvdCBtb2RpZmllZCBpbiB0cmFuc2l0LgoKQXQgdGhlIHNhbWU ...
DKIM-Domain: sender.example
DKIM-Identity: @sender.example
DKIM-Selector: testkey
Arrival-Date: 8 Oct 2011 20:15:58 +0000 (GMT)
Source-IP: 192.0.2.1
Reported-Domain: a.sender.example
```

```
Reported-URI: http://www.sender.example/

--------------Boundary-00=_3BCR4Y7kX93yP9uUPRhg
Content-Type: text/rfc822-headers
Content-Transfer-Encoding: 7bit

Authentication-Results: mta1011.mail.tp2.receiver.example;
 dkim=fail (bodyhash) header.d=sender.example;
 spf=pass smtp.mailfrom=anexample.reply@a.sender.example
Received: from smtp-out.sender.example
 by mta1011.mail.tp2.receiver.example
 with SMTP id oB85W8xV000169;
 Sat, 08 Oct 2011 13:15:58 -0700 (PDT)
DKIM-Signature: v=1; c=relaxed/simple; a=rsa-sha256;
 s=testkey; d=sender.example; h=From:To:Subject:Date;
 bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
 b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB
 4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut
 KVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV
 4bmp/YzhwvcubU4=
Received: from mail.sender.example
 by smtp-out.sender.example
 with SMTP id o3F52gxO029144;
 Sat, 08 Oct 2011 13:15:31 -0700 (PDT)
Received: from internal-client-001.sender.example
 by mail.sender.example
 with SMTP id o3F3BwdY028431;
 Sat, 08 Oct 2011 13:15:24 -0700 (PDT)
Date: Sat, 8 Oct 2011 16:15:24 -0400 (EDT)
Reply-To: anexample.reply@a.sender.example
From: anexample@a.sender.example
To: someuser@receiver.example
Subject: You have a new bill from your bank
Message-ID: <87913910.1318094604546@out.sender.example>

--------------Boundary-00=_3BCR4Y7kX93yP9uUPRhg--
```

Le but de l'authentification du courrier électronique étant d'améliorer la sécurité, il n'est pas étonnant que la section 6, considérée aux problèmes de sécurité, soit particulièrement détaillée. Quelques points à garder en tête, donc. Par exemple, les rapports ARF eux-même peuvent être des faux. Il ne faut agir de manière automatique sur un de ces rapports que s'ils ont été authentifiés d'une manière ou d'une autre. Ensuite, générer automatiquement des rapports ARF peut ouvrir une voie à l'attaque par déni de service : un méchant pourrait envoyer plein de messages délibèrement faux, pour déclencher l'émission massive de rapports ARF.

Il existe apparemment déjà au moins un générateur d'ARF qui gère cette extension. PayPal et Hotmail ont déjà annoncé leur intention de l'utiliser.