RFC 3797 : Publicly Verifiable Nominations Committee (NomCom) Random Selection

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 juillet 2006. Dernière mise à jour le 25 juin 2014

Date de publication du RFC : Juin 2004

https://www.bortzmeyer.org/3797.html

Comment faire un tirage au sort dont tout le monde puisse vérifier la sincérité ? C'est à ce problème que s'attaque ce RFC. Il a des applications pratiques, notamment pour la désignation d'un des groupes de l'IETF, le NomCom.

L'approche classique du tirage au sort est de désigner une ou plusieurs personnes supposées dignes de confiance. Ces personnes vont superviser le tirage. On voit ainsi souvent des affirmations du genre « Tirage contrôlé par huissier ». Outre son coût, les faiblesses de ces méthode sont que la personne qui supervise n'est pas forcément digne de la confiance qu'on met en elle et, surtout, que cette personne peut être trompée par l'organisateur. Par exemple, si le tirage est effectué par un logiciel, comment diable l'huissier va-t-il s'assurer que le logiciel est neutre ? Même s'il a les sources et que l'huissier est en plus informaticien, il serait trivial de le tromper (le fameux article de Thompson, "*Reflections on Trusting Trust*" <http://www.acm.org/classics/sep95/> explique bien comment).

Notre RFC propose une solution qui est bien plus dans l'esprit de l'Internet : permettre à chacun de vérifier que le tirage est honnête. Le principe est simple : on désigne à l'avance une série de sources de hasard, comme la quantité de transactions à une Bourse ou bien le résultat d'une loterie d'État et on utilise ces sources comme entrée d'une fonction de hachage, qui va produire un nombre aléatoire, que chacun pourra vérifier (puisque les sources de hasard et l'algorithme utilisé sont publics).

La bonne dispersion fournie par la fonction de hachage fait que l'algorithme fonctionne même si l'une des sources de hasard est de médiocre qualité.

Le RFC détaille les qualités qu'on attend d'une bonne source de hasard. Elle doit évidemment être publique, mais il faut aussi qu'elle ne puisse pas être influencée facilement, ce qui conduit, pour la Bourse, à préférer le nombre de transactions au cours des actions, plus influençables.

Cette technique est utilisée par exemple pour la désignation du NomCom ("*Nominating Committee*", décrit dans le RFC 7437 [1]), comité tiré au hasard parmi des volontaires et qui désigne les membres de l'IAB. Elle a aussi été utilisée par l'ICANN, pour choisir le préfixe (ce fut `xn`) des noms de domaines internationalisés, afin d'éviter tout cybersquatting préventif (voir la méthode <http://www.ietf.org/mail-archive/web-old/ietf-announce-old/current/msg22384.html> et l'annonce du résultat <http://www.ietf.org/mail-archive/web-old/ietf-announce-old/current/msg22565.html>).

Voici par exemple les paramètres sélectionnés pour le NomCom de l'IETF (tirage du 6 juillet 2014) :

```
Date: Fri, 20 Jun 2014 11:20:28 -0700
From: NomCom Chair 2014 <nomcom-chair-2014@ietf.org>
To: IETF Announcement List <ietf-announce@ietf.or>
Subject: NOMCOM 2014 random seed selection

As per RFC3777, and using the RFC3797,
   Publicly Verifiable Nominations Committee (NomCom) Random Selection

the following are the seed selection that will be used on 2014-07-06.

Seeds:
-------
The following are the seed sources (in order) that will be used in
selecting the 2014-15 NomCom members:

Canadian Lottery Lotto 649
Wednesday, July 2, 2014 Results:
http://lotoquebec.com/loteries/nav/en/draw-games/lotto-6-49/results-past-year#2014-07-02
  (7 numbers including the bonus number: numbers between 1 and 49)

US National debt ("Debt Held by the Public"), published by the
Treasury department as of Thursday, July 7, 2014
http://www.treasurydirect.gov/NP/BPDLogin?application=np
http://www.treasurydirect.gov/NP/debt/search?startMonth=07&startDay=7&startYear=2014&endMonth=&endDay=&endYe
  Last 8 digits, ignore the commas and periods

US National debt ("Intragovernmental Holdings"), published by the
Treasury department as of Thursday, July 7, 2014
http://www.treasurydirect.gov/NP/BPDLogin?application=np
http://www.treasurydirect.gov/NP/debt/search?startMonth=07&startDay=7&startYear=2014&endMonth=&endDay=&endYe
  Last 8 digits, ignore the commas and periods

Euromillions Lottery
Friday July 5, 2014 Results:
http://www.europeanlotteryguild.com/lottery_results/euromillions_results/
http://www.europeanlotteryguild.com/lottery_results/euromillions_results/draw_history?results_date=2014-07-0
  (7 numbers including the star balls: 5 numbers between 1 and 50 and 2
   star balls between 1 and 11)

All the above seeds will be provided (in the order listed above) as
input to the RFC 3797 selection algorithm to determine the ten
voting members of the 2014-15 Nomcom.
```

Notez qu'il y avait deux erreurs, sur la date des Euromillions (le 5 est un samedi...) et sur celle de la dette nationale états-unienne :-)

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7437.txt`