RFC 7070 : An Architecture for Reputation Reporting

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 novembre 2013

Date de publication du RFC : Novembre 2013

http://www.bortzmeyer.org/7070.html

Il y a des tas de fois dans l'Internet où on souhaite se renseigner automatiquement sur la réputation d'une entité (une adresse IP, un nom de domaine, etc). Aujourd'hui, chaque application qui souhaite le faire développe une technologie spécifique pour l'accès à cette réputation (comme les listes noires DNS du RFC 5782 [1]). L'idée du projet repute <http://tools.ietf.org/wg/repute> de l'IETF est de créer des mécanismes communs, utilisables par une variété d'applications. Ce premier RFC est la fondation du projet et décrit l'architecture générale du système de réputation. D'autres RFC vont décrire les détails.

Un des principes fondateurs de l'Internet est qu'on n'a pas besoin de montrer patte blanche avant d'accéder à un service. Par exemple, pour une des applications les plus répandues, le courrier électronique, n'importe qui peut écrire à n'importe qui sans introduction préalable. On entend souvent des gens qui n'ont pas réfléchi à la question dire que cela contribue aux problèmes de sécurité de l'Internet. Mais cela a surtout contribué à son succès ! Comme le note à juste titre le RFC 5218, un système plus rigide, avec mécanismes de sécurités dès le début, avec authentification obligatoire avant d'envoyer un message, plairait certes aux dirigeants chinois ou saoudiens, et permettrait certainement de mieux traiter certains problèmes comme le spam. Mais il aurait aussi certainement à coup sûr tué le courrier électronique avant même qu'il ne décolle (ce n'est pas un avis personnel : c'est une constatation fondée sur l'observation de systèmes concurrents, bien oubliés aujourd'hui).

Donc, la plupart des services de l'Internet n'authentifient pas (l'émetteur d'un courrier peut mettre ce qu'il veut dans le champ `From:`...) et, même lorsqu'ils le font (en cas d'utilisation de TCP, l'adresse IP est relativement authentifiée), l'authenticité d'un pair ne nous renseigne pas sur son honnêteté et sa sincérité <http://www.bortzmeyer.org/authentifier-et-autoriser.html>. Cette confusion entre authentification et autorisation est très fréquente, elle a même mené certains spammeurs à être les premiers

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5782.txt

à déployer certaines techniques (comme DKIM), en espérant jouer sur cette confusion. Si certains administrateurs de serveurs de messagerie étaient assez bêtes pour retirer des points de « spamicité » uniquement parce qu'un message avait une signature DKIM valide, le spammeur pouvait espérer injecter quelques spams en plus.

Résultat, les services de l'Internet, comme le courrier électronique, sont un grand succès mais, suite logique de ce succès, sont affligés de nombreux problèmes de sécurité (« "*Any real ecosystem has parasites*" », dirait Cory Doctorow). Comment lutte-t-on contre ces problèmes ? Une méthode courante est d'utiliser la **réputation**, c'est-à-dire des affirmations par un tiers comme quoi telle ou telle entité est digne de confiance. Son utilisation est particulièrement courante dans le cadre de la lutte contre le spam : on demande à un service de réputation « cette adresse IP est-elle souvent émettrice de spam ? » Si oui, on peut décider de ne pas accepter son message. Cette fois, on ne se limite pas à l'authentification : on bâtit au-dessus d'elle.

Si le monde du courrier électronique fut le premier à utiliser à grande échelle ces systèmes de réputation, d'autres dans l'Internet pourraient y venir. C'est pour les aider qu'a été développé ce modèle, et les protocoles qui l'accompagnent. En effet, les mécanismes actuels (le plus connu étant les DNSBL décrites dans le RFC 5782 mais il y a aussi le système du RFC 5518 pour se porter garant) sont très simplistes, notamment par le fait que leur réponse est binaire. On aurait besoin de nuances, et de la capacité d'apporter des détails (le RFC cite comme exemple la différence entre « approuver un chèque » et une institution très typiquement états-unienne, « faire un "*credit report*" complet »). Autre exemple où les systèmes actuels sont insuffisants, le cas où un acteur a une réputation différente selon ses services. Par exemple, un site de commerce en ligne peut avoir une mauvaise réputation pour les délais de livraison, mais un bonne réputation pour la qualité de l'information qu'il donne en cas de problème.

Compte tenu de tous ces points, le groupe de travail a développé un modèle, qui est résumé en section 2 de ce RFC. La réputation se gère à trois. On a un acteur qu'on veut évaluer, désigné par un **identificateur**. Un **client** qui est intéressé par la réputation de cet acteur. Et un **service de réputation** qui va distribuer de l'information sur les acteurs. Le service de réputation peut être public ou accessible seulement à des abonnés. Le client devra être configuré pour accéder à ce service de réputation. Les identificateurs utilisés peuvent être variés : noms de domaine, adresses de courrier électronique, adresses IP, etc.

Descendons un peu plus dans les détails (sections 4 à 6). L'architecture du système est celle d'un simple protocole question/réponse, qui peut utiliser comme transport sous-jacent divers mécanismes comme par exemple HTTP, le DNS... La syntaxe exacte dépend de l'application (rappelez-vous que ce RFC ne décrit qu'un cadre général). Un format possible des informations de réputation est normalisé dans le RFC 7071, un des protocoles d'accès, fondé sur HTTP, est dans le RFC 7072, et les identificateurs utilisés dans le cas du courrier électronique sont dans le RFC 7073.

Prenons l'exemple d'une application, un logiciel qui reçoit le courrier électronique, et qui utilise DKIM (RFC 6376) pour authentifier le domaine expéditeur. Ce nom étant authentifié, elle pourra s'en servir comme base de l'évaluation du message : on authentifie l'envoyeur du courrier avec DKIM, on interroge un serveur de réputation sur la réputation de cet envoyeur, et on décide alors d'accepter le message ou de l'envoyer dans le dossier « Spam ». DKIM apporte l'authentification, le système de notre RFC ajoute la réputation, et les deux ensemble permettent l'autorisation.

Que retourne un serveur de réputation ? Trois choses importantes :

— Le nom de l'entité qu'il vient d'évaluer (dans l'exemple précédent, ce pourrait être `gmail.com`, le domaine expéditeur qui signe avec DKIM).

— Une (ou plusieurs) assertion(s). Une assertion est une affirmation, plus ou moins fausse, sur le comportement de l'entité. Pour un domaine expéditeur, cela pourrait être « envoie du spam ». Pour un site de commerce en ligne, « livre dans les temps ». Pour quelqu'un qui modifie Wikipédia, « vandalise des articles <https://fr.wikipedia.org/wiki/Aide:Vandalisme> ».
— Un classement. Contraitrement aux DNSBL, le système de réputation n'est pas binaire. Une assertion peut être plus ou moins fausse et c'est ce qu'exprime le classement. Un classement va de 0 (assertion complètement fausse) à 1 (assertion toujours vraie). Ainsi, un domaine qui envoie rarement du spam pourrait avoir un classement de 0,2 à l'assertion « envoie du spam » alors qu'un domaine plus spammeur aurait un classement de 0,6.

Rappelez-vous que les assertions pertinentes, ainsi que la signification des classements, dépendent de l'application. Chaque application (réception de courrier, jugement des commentaires sur un blog, etc) aura donc sa propre spécification, décrivant les réponses attendues. Les applications ainsi spécifiées sont stockées dans un registre IANA <https://www.iana.org/assignments/reputation-parameters/reputation-parameters.xhtml#applications>.

La réponse structurée est dans un objet nommé « **reputon** ». Les détails de sa syntaxe dépendent du transport utilisé et de l'application. Mais si vous voulez voir des exemples de reputons, regardez le RFC 7071.

Pour obtenir un reputon en réponse, le client aura dû envoyer le nom de l'entité qu'il veut évaluer, le nom de l'application (tiré du registre IANA cité plus tôt) et, éventuellement, les assertions qui l'intéressent (le serveur de réputation peut en stocker plusieurs pour une même entité).

Comme le note la section 8, tout ceci peut poser des problèmes de préservation de la vie privée. Les informations de réputation peuvent dans certains cas être considérées sensibles et pas distribuables publiquement. Et il n'y a pas que la réponse qui peut être sensible, la question l'est aussi parce qu'elle révèle un intérêt du client (« le MP3 tina-turner-total-eclipse-of-the-heart.mp3 de condensat SHA-256 5ba214e312254abd22e7aae38af865a92f93cbd01e180051ab5bd443ceeae594, que je m'apprête à télécharger, est-il de bonne qualité ? ») Le RFC insiste donc sur la nécessité de fournir de la confidentialité si les données le justifient. Par exemple, le DNS, qui ne fournit aucune confidentialité, ne doit en aucun cas être utilisé pour des services sensibles. Si on se sert de HTTP comme transport de données de réputation sensibles, il faut utiliser HTTPS et, si on se sert du courrier, PGP ou équivalent.

De même, un accès non autorisé à la base de données d'un serveur de réputation pourrait causer des dommages, si ces données sont privées.

Mais il y a aussi des problèmes de sécurité qui ne sont pas liées à la vie privée (section 9). Par exemple, que se passe t-il si le serveur de réputation ment, distribuant délibérement des informations trop ou pas assez favorables à certaines entités ? Si un client accède à des informations de réputation, c'est probablement pour s'en servir pour prendre des décisions et des informations fausses peuvent donc avoir des conséquences concrètes désagréables. Imaginez un serveur de courrier qui accepterait du spam (ou, au contraire, rejetterait des messages légitimes) parce que le serveur de réputation l'a trompé.

Il n'y a pas de solution miracle à ce problème. Utiliser un serveur de réputation, c'est sous-traiter, c'est faire confiance. Cela implique le risque d'être trompé. Au minimum, le RFC conseille de ne faire confiance qu'à des services de réputation qui publient leurs pratiques de classement, qu'on puisse les analyser (voir le RFC 6471 pour ce problème dans le cas des listes noires de spammeurs dans le DNS).

Les motivations pour le projet de réputation ont été décrites dans les supports de la première présentation à l'IETF <http://www.ietf.org/proceedings/81/slides/repute-0.pdf>.

Pour des exemples d'utilisation et des informations sur les mises en œuvre de ce système, voir mes articles sur le RFC 7071 et sur le RFC 7072. Merci à Murray S. Kucherawy pour son aide.