RFC 5039 : The Session Initiation Protocol (SIP) and Spam

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 janvier 2008

Date de publication du RFC : Janvier 2008

https://www.bortzmeyer.org/5039.html

Le spam est la plaie du courrier électronique. Peut-il également affecter d'autres services comme la téléphonie sur IP ? C'est la crainte de l'IETF, d'où ce RFC qui étudie les moyens de faire face au spam via le protocole SIP, avant que ce phénomène se développe.

Rien n'indique que le spam restera limité au courrier électronique. Au contraire, l'expérience semble indiquer que, du moment qu'une technique permet de joindre beaucoup de personnes pour pas cher, et sans introduction préalable, elle est utilisée par les spammeurs. Les techniques soi-disant « sans spam » sont uniquement celles qui ne sont peu ou pas utilisées, ou qui sont chères et peu pratiques.

Le message principal du RFC est qu'il faut s'y prendre à l'avance. Le spam aurait été plus facile à combattre si on avait déployé certaines techniques dès le début. Pour le protocole SIP (RFC 3261 [1]), de loin le principal protocol ouvert pour faire du multimédia, notamment de la téléphonie, sur Internet, il est donc peut-être encore temps d'agir. (Je suis personnellement prudent par rapport à cette affirmation. Pour le courrier électronique, je n'ai pas encore vu de solution qui, si elle avait été déployée plus tôt, aurait empêché le spam de prendre une telle ampleur.)

La section 2 explique les formes que pourrait prendre le spam avec SIP. Elle note qu'il n'est pas forcément nécessaire d'envoyer un message pour spammer. Par exemple, SIP a une méthode INVITE qui peut prendre un en-tête `Subject:` (section 20.36 du RFC 3261). Si ce sujet est affiché à l'utilisateur avant même qu'il n'accepte l'appel (ce que font certains "*soft phones*"), il peut servir de canal pour le spam.

Cette particularité de SIP, et quelques autres, font que certaines des techniques couramment utilisées pour le filtrage du courrier ne sont pas forcément efficaces. Ainsi, le filtrage par contenu (section 3.1 de

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc3261.txt`

notre RFC), comme les filtres bayésiens, n'est pas tellement appliquable dans le cas d'un message audio, encore moins pour un message vidéo.

Le RFC insiste sur importance de l'**identité**. Beaucoup de techniques marchent si on peut être à peu près certain de l'identité de l'émetteur. Par exemple, les listes blanches sont facilement prises en défaut si le spammeur peut se faire passer pour une personne connue. Le problème est d'autant plus difficile qu'on voudrait authentifier la personne, pas uniquement son ordinateur car, comme le note la section 3.3, si l'ordinateur est compromis et est devenu un zombie, l'authentifier ne servira à rien.

Un autre problème classique des listes blanches est le fait qu'elles ne gèrent que le cas des personnes proches. Le RFC propose dans sa section 3.5, d'utiliser les mécanismes de **réseau social** (≪ mes copains ont aussi des copains ≫) pour augmenter automatiquement les listes blanches (la plupart des logiciels SIP, comme les logiciels d'IM, ont un système analogue, en général nommé "*buddy list*", liste des copains).

En revanche, les techniques de dissimulation d'adresses, comme on voit pour le courrier (`stephane plus blog à bortzmeyer point org`) ne fonctionnent pas bien si on reste aux traditionnels numéros de téléphone. L'espace possible est en effet restreint et relativement facile à parcourir de manière exhaustive (ENUM facilitera probablement les choses pour les spammeurs).

Les approches du problème peuvent aussi être basées, non pas sur une technique mais sur une organisation. Une architecture possible est décrite en section 3.13, avoir un petit nombre de fournisseurs SIP qui se transmettent des coups de téléphone entre eux, et n'en acceptent pas des autres fournisseurs. Un tel cartel, qui ressemble aux propositions de "*mail peering*" qui sont proposées pour le courrier par des organismes comme le MAAWG ou comme le FAI AOL aurait, note notre RFC, tous les avantages et tous les inconvénients de l'actuel réseau téléphonique, que SIP visait à remplacer.

Finalement, la section 6 du RFC est consacrée aux quatre recommendations importantes :
— Développer un système d'identité fort, comme décrit dans le RFC 4474.
— Utiliser largement les listes blanches.
— Résoudre le problème de l'**introduction**. Si tout le monde utilise des listes blanches, on risque de ne pas pouvoir appeler quelqu'un à qui on n'a pas été **introduit**. Les mécanismes d'introduction visent à résoudre ce problème, par exemple via les réseaux sociaux (≪ les amis de mes amis sont mes amis ≫).
— Ne pas attendre que le spam se soit répandu (voir le début de cet article).