

RFC 5379 : Guidelines for Using the Privacy Mechanism for SIP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 Février 2010

Date de publication du RFC : Février 2010

<http://www.bortzmeyer.org/5379.html>

Le protocole SIP, surtout connu pour son rôle dans la téléphonie sur IP, dispose de plusieurs fonctions permettant de protéger la vie privée de ses utilisateurs. Spécifiées dans plusieurs RFC, ces fonctions ne sont pas forcément évidentes à utiliser, d'où ce RFC qui tente de guider les développeurs vers les bonnes pratiques.

SIP est normalisé dans le RFC 3261¹ et est certainement le premier protocole de téléphonie sur IP, d'autant plus que certains de ses concurrents, bâtis sur des protocoles fermés, ne respectent pas forcément la vie privée de leurs utilisateurs. Et SIP, qu'en fait-il ? Certaines de ces fonctions peuvent être excessivement intrusives, par exemple le fait que l'adresse de l'appelant soit fournie, et il existe donc des moyens de les débrayer.

Le cadre général est donné dans le RFC 3323. Il introduit par exemple l'idée de mettre `sip:anonymous@anonymous.i` comme adresse de l'appelant, même le simple nom de domaine pouvant révéler des informations (section 4.1.1.3 du RFC 3323 et section 5.1.4 de notre RFC). Les RFC 3325 et RFC 4244 fournissent des méthodes supplémentaires.

Qu'apporte notre RFC 5379 ? Il ne change aucun protocole, il explique simplement comment mieux utiliser les extensions de maintien de la vie privée décrites dans les RFC précédents. C'est donc un bon point de départ si on écrit un logiciel SIP soucieux de vie privée. Ainsi, le tableau de la section 4.1 résume de manière simple les actions qui doivent être menées (ou pas) par les différents agents, selon le niveau de protection demandé par l'utilisateur (ces niveaux avaient été définis dans la section 4.2 du RFC 3323). Par exemple, les en-têtes `Via:` (section 8.1.1.7 du RFC 3261) indiquent l'endroit où envoyer des réponses, donc où se trouve l'appelant. Au niveau "header" de protection de la vie privée, ils doivent

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

donc être « anonymisés », c'est-à-dire remplacés par un en-tête `Via` : d'un relais (section 5.1 du RFC 3323 et 5.1.15 de notre RFC).

De même, la section 4.3 rappelle nettement le rôle de l'option "*critical*" dans un en-tête `Privacy` : . Elle indique que l'appelant préfère que l'appel avorte plutôt que de transmettre des informations privées (certains appelés refusent les appels où certaines informations manquent et "*critical*" sert à indiquer s'il faut accepter leurs exigences ou pas). Le RFC 3323 était nettement moins directif sur cette option.

La section 5 résume le traitement de chaque en-tête sensible, lorsque l'utilisateur demande le service de protection de la vie privée. Ainsi, `Contact` : (section 5.1.3) est un cas délicat car il doit être un URI qui pointe réellement sur quelque chose (il sert à contacter le logiciel de l'utilisateur). S'il est remplacé, il doit donc l'être par un URI qui marche, par exemple un système de relais de courte durée de vie.

Certains en-têtes, moins utiles au fonctionnement de SIP, sont traités plus violemment. C'est ainsi que la section 5.1.13 recommande d'éliminer l'en-tête `Subject` : car elle peut être trop révélatrice. Même chose pour `User-Agent` : (section 5.1.14) qui indique le type de logiciel utilisé et qui peut donc révéler des choses sur son propriétaire.