Groupe de travail Réseau
Request for Comments : 5363
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

G. Camarillo, Ericsson
A.B. Roach, Tekelec

octobre 2008

Cadre et considérations sur la sécurité pour les services de liste d'URI du protocole d'initialisation de session (SIP)

Résumé
Le présent document décrit le besoin des services de liste d'URI *(Uniform Resource Identifier, identifiant de ressource universel)* de SIP et fournit les exigences pour leur invocation. Il définit de plus un cadre pour les services de liste d'URI de SIP, qui inclut les considérations sur la sécurité applicables à ces services.

Table des matières

1. Introduction

Certaines applications exigent que, à un moment donné, un agent d'utilisateur SIP [RFC3261] (UA, *User Agent*) effectue une transaction similaire avec un certain nombre d'UA distants. Par exemple, une application de messagerie instantanée qui a besoin d'envoyer un message particulier (par exemple, "Salut les gars") à n receveurs a besoin d'envoyer n demandes MESSAGE ; une à chaque receveur.

Quand la transaction qui doit être répétée consiste en grandes demandes, ou quand le nombre de receveurs est élevé, ou les deux, le réseau d'accès de l'UA doit porter une quantité de trafic considérable. Mener à bien toutes les transactions sur un accès à faible bande passante exigerait beaucoup de temps. Ceci est inacceptable pour un certain nombre d'applications.

Une solution à ce problème consiste à introduire des services de liste d'URI dans le réseau. La tâche d'un service de liste d'URI SIP est de recevoir une demande qui contient ou fait référence à une liste d'URI (c'est-à-dire, une liste d'un ou plusieurs URI) et d'envoyer des demandes similaires aux destinations de cette liste. Une fois les demandes envoyées, le

service de liste d'URI informe normalement l'UA de leur état. Effectivement, le service de liste d'URI se comporte comme un agent d'utilisateur de boucle locale (B2BUA, *Back-to-Back-User-Agent*).

Un service de liste d'URI peut prendre en entrée une liste d'URI contenus dans la demande SIP envoyée par le client ou une liste d'URI externe (par exemple, l'URI de demande est un URI SIP associé à une liste d'URI au serveur). Les listes d'URI externes sont normalement établies en utilisant des mécanismes hors bande (par exemple, le protocole d'accès à la configuration XML (XCAP, *XML Configuration Access Protocol*) [RFC4825]). Un exemple de service de liste d'URI pour les demandes SUBSCRIBE qui utilise des listes d'URI mémorisés est décrit dans la [RFC4662].

Le reste de ce document donne les exigences et un cadre pour les services de liste d'URI utilisant des listes d'URI contenues dans les demandes, des listes d'URI externes, ou les deux.

2. Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

3. Exigences

Le paragraphe 3.1 discute des exigences qui s'appliquent seulement aux services de liste d'URI qui utilisent les listes contenues dans la demande, et le paragraphe 3.2 discute les exigences qui s'appliquent aussi aux services qui utilisent des listes externes.

3.1 Exigences pour les services de liste d'URI utilisant des listes contenues dans la demande

REQ 1 : Le mécanisme d'invocation du service de liste d'URI DOIT permettre à l'invocateur de fournir une liste des URI de destination au service de liste d'URI.

REQ 2 : Le mécanisme d'invocation NE DEVRAIT PAS exiger plus d'une transaction.

3.2 Exigences générales pour les services de liste d'URI

GEN 1 : Un service de liste d'URI PEUT inclure des services au delà de l'envoi de demandes aux URI de la liste d'URI. C'est-à-dire, les services de liste d'URI peuvent être modélisés comme des serveurs d'application. Par exemple, un service de liste d'URI traitant des demandes INVITE peut se comporter comme un serveur de conférence et effectuer un mélange de supports pour tous les participants.

GEN 2 : L'interprétation de la signification de la liste d'URI envoyée par l'invocateur DOIT être à la discrétion de l'application à laquelle la liste est envoyée.

GEN 3 : Il DOIT être possible à l'invocateur de trouver le résultat des opérations effectuées par le service de liste d'URI avec la liste d'URI. Un invocateur peut, par exemple, être intéressé par l'état des transactions initiées par le service de liste d'URI.

GEN 4 : Les services de liste d'URI NE DOIVENT PAS envoyer de demandes à une destination sans authentifier l'invocateur.

4. Cadre

Ce cadre ne se restreint pas aux serveurs d'application qui fournissent seulement des services de ventilation des demandes. Selon GEN 1, ce cadre traite aussi des serveurs d'application qui fournissent un service particulier incluant la ventilation des demandes (par exemple, un serveur de conférence qui envoie des INVITE à plusieurs participants choisis par un agent d'utilisateur).

4.1 Portage des listes d'URI dans SIP

Les exigences relatives aux services de liste d'URI qui utilisent des listes contenues dans la demande identifient le besoin d'un mécanisme pour fournir un service de liste d'URI SIP avec une liste d'URI dans une seule transaction. On définit un nouveau type de disposition [RFC2183] pour le champ d'en-tête Content-Disposition : recipient-list *(liste de receveurs)*. Les demandes et les réponses PEUVENT porter des corps recipient-list. Les corps dont le type de disposition est recipient-list portent une liste des URI qui contiennent le receveurs finaux des demandes à générer par un service de liste d'URI.

Le format par défaut des corps recipient-list est spécifique du service. Donc, les spécifications de services de liste d'URI DOIVENT spécifier un format par défaut pour les corps recipient-list utilisés dans un service particulier. Dans tous les cas, les clients NE DEVRAIENT PAS inclure d'URI particulier plus d'une fois dans une liste d'URI donnée.

Un serveur d'UA qui reçoit une demande avec plus d'une partie de corps recipient-list (par exemple, chaque partie de corps utilisant un format de liste d'URI différent) DOIT se comporter comme si il avait reçu une seule liste d'URI contenant tous les URI présents dans les différentes parties de corps.

Un serveur d'UA qui reçoit une liste d'URI recipient-list qui contient un URI plus d'une fois DOIT se comporter comme si cet URI apparaissait juste une fois dans la liste d'URI. Le serveur d'UA utilise les règles de comparaison spécifiques du schéma d'URI de chacun des URI de la liste d'URI pour déterminer si il y a un URI qui apparaît plus d'une fois. De plus, la Section 4 de "Extension de format du langage de balisage extensible (XML) pour la représentation des attributs de contrôle de copie dans les listes de ressources" [RFC5364] discute des cas où des entrées d'URI dupliquées sont étiquetées avec des valeurs différentes de l'attribut "copyControl". Naturellement, les services de liste d'URI qui utilisent l'attribut "copyControl" défini dans la [RFC5364] doivent suivre les recommandations de la [RFC5364] à l'égard de l'évitement d'envoi de demandes dupliquées.

La façon dont un serveur d'UA interprète une liste d'URI reçue est spécifique du service, comme décrit au paragraphe 4.2.

4.2 Traitement des listes d'URI

Conformément à GEN 1 et GEN 2, les services de liste d'URI peuvent se comporter comme des serveurs d'application. C'est-à-dire, en prenant une liste d'URI en entrée, ils peuvent fournir des services arbitraires. Donc, l'interprétation de la liste d'URI par le serveur dépend du service à fournir. Par exemple, pour un serveur de conférence, les URI de la liste peuvent identifier l'ensemble initial de participants. Par ailleurs, pour un serveur qui traite des demandes MESSAGE, les URI de la liste peuvent identifier les receveurs d'un message instantané.

Au niveau de SIP, cela implique que le comportement des serveurs d'application qui reçoivent des demandes avec des listes d'URI DEVRAIT être spécifié par service. Des exemples de telles spécifications sont la [RFC5366] pour INVITE, la [RFC5365] pour MESSAGE, et la [RFC5367] pour SUBSCRIBE.

4.3 Résultats

En accord avec GEN 3, les agents d'utilisateur devraient avoir un moyen d'obtenir des informations sur les opérations effectuées par le serveur d'application. Comme ces opérations sont spécifiques du service, la façon dont les agents d'utilisateur sont informés est aussi spécifique du service. Par exemple, un agent d'utilisateur qui établit une conférence ad hoc avec un INVITE et une liste d'URI peut découvrir quels participants ont été intégrés avec succès à la conférence en utilisant le paquetage de conférence [RFC4575].

5. Considérations sur la sécurité

La sécurité joue un rôle important dans la mise en œuvre de tout service de liste d'URI. En fait, c'est la plus importante zone commune parmi tous les types de services de liste d'URI.

Par définition, un service de liste d'URI prend une demande et en envoie un nombre potentiellement grand. Des attaquants peuvent tenter d'utiliser les services de liste d'URI comme amplificateurs de trafic pour lancer des attaques de déni de service (DoS, *denial-of-service*). Cette section donne des lignes directrices sur la façon d'éviter ces attaques.

5.1 Intégrité et confidentialité de liste

Des attaquants peuvent tenter de modifier les listes d'URI envoyées des clients aux serveurs. Cela va causer au serveur un comportement différent de celui attendu par le client (par exemple, les demandes étant envoyées à des receveurs différents de ceux spécifiés par le client). Pour empêcher cette attaque, les clients DEVRAIENT protéger l'intégrité des listes d'URI en utilisant des mécanismes de bout en bout comme S/MIME ou, si ce n'est pas disponible, des mécanismes bond par bond comme TLS. S/MIME et TLS peuvent tous deux fournir aussi la confidentialité de liste d'URI si nécessaire.

5.2 Attaques d'amplification

Les services de liste d'URI prennent une demande et en envoient un nombre potentiellement grand. Étant donné que les services de liste d'URI sont normalement mis en œuvre par dessus des serveurs puissants avec des liaisons d'accès à haut débit, on devrait veiller à empêcher des attaquants de les utiliser comme outils d'amplification pour lancer des attaques de DoS.

Des attaquants peuvent tenter d'envoyer une liste d'URI contenant des URI dont la partie hôte achemine sur les victimes de l'attaque de DoS. Ces victimes n'ont pas besoin d'être des nœuds SIP ; elles peuvent être des points d'extrémité non SIP ou même des routeurs. Si cette attaque réussit, son résultat est qu'un attaquant peut inonder un ensemble de nœuds, ou un seul nœud, avec du trafic sans avoir besoin de générer lui-même un gros volume de trafic.

Dans tous les cas, on notera que ce problème n'est pas spécifique des services de liste d'URI de SIP ; il apparaît aussi dans des scénarios qui se rapportent au multi rattachement où un serveur doit contacter un ensemble d'adresses IP fournies par un client.

Il y a plusieurs mesures qui doivent être prises pour prévenir ce type d'attaque. La première est d'empêcher les utilisateurs non autorisés d'utiliser les services de liste d'URI. Donc, les services de liste d'URI NE DOIVENT PAS effectuer d'explosion de demandes pour un utilisateur non autorisé. Les services de liste d'URI DOIVENT authentifier les utilisateurs et vérifier si ils sont autorisés à demander le service avant d'effectuer aucune ventilation de demandes.

Noter que le risque de cette attaque existe aussi quand un client utilise des listes d'URI mémorisées. Les serveurs d'application DOIVENT utiliser des mécanismes d'authentification et d'autorisation avec des propriétés de sécurité équivalentes quand ils traitent les listes d'URI mémorisées et contenues dans la demande.

Même si la règle précédente empêche les utilisateurs non autorisés d'utiliser les services de liste d'URI, les utilisateurs autorisés peuvent quand même lancer des attaques utilisant ces services. Pour empêcher ces attaques, on introduit le concept des listes d'inclusion *(opt-in)*. C'est-à-dire, les services de liste d'URI ne devraient pas permettre à un client de placer un utilisateur (identifié par son URI) dans une liste d'URI si il n'a pas accepté au préalable d'être placé dans une telle liste d'URI. Donc, les services de liste d'URI NE DOIVENT PAS envoyer de demande à une destination qui n'a pas accepté préalablement de recevoir des demandes provenant du service de liste d'URI. Les utilisateurs peuvent accepter de recevoir des demandes provenant d'un service de liste d'URI de plusieurs façons, comme de remplir une page de la Toile, d'envoyer un message, de signer un contrat, ou d'utiliser le "Cadre des communications fondées sur le consentement dans SIP" [RFC5360], dont les exigences sont discutées dans la [RFC4453]. De plus, les utilisateurs DOIVENT être capables de décrire plus en détails les demandes qu'ils veulent recevoir. Par exemple, un usager peut vouloir recevoir seulement des demandes provenant d'un service de liste d'URI particulier au nom d'un utilisateur particulier. Effectivement, ces règles font des listes d'inclusion des listes d'URI qui sont utilisées par des services de liste d'URI.

Quand un service de liste d'URI reçoit d'un client une demande avec une liste d'URI, le service de liste d'URI vérifie si toutes les destinations ont accepté préalablement de recevoir des demandes provenant du service au nom de ce client. Si la liste d'URI a la permission d'envoyer des demandes à toutes les cibles de la demande, il le fait. Sinon, il n'envoie aucune demande.

Le cadre des communications fondées sur le consentement dans SIP [RFC5360] spécifie un moyen pour que le service de liste d'URI informe le client que des permissions manquaient et comment les demander.

Noter que le mécanisme utilisé pour obtenir les permissions ne devrait pas créer d'opportunités de lancer des attaques d'amplification de DoS. Ces attaques seraient possibles si, par exemple, le service de liste d'URI contactait automatiquement tout l'ensemble de cibles pour lequel il n'avait pas de permissions afin de demander les permissions. Le service de liste d'URI recevrait une demande SIP et enverrait un certain nombre de messages de demande d'autorisation. Le cadre des communications fondées sur le consentement dans SIP [RFC5360] évite ce type d'attaque en faisant que le client génère en gros la même quantité de trafic vers le service de liste d'URI que ce que le service génère vers les destinations.

Afin d'avoir un moyen interopérable de satisfaire les exigences relatives aux listes d'inclusion décrites dans cette section, les services de liste d'URI DOIVENT mettre en œuvre et DEVRAIT utiliser le "Cadre des communications fondées sur le consentement dans le protocole d'initialisation de session" [RFC5360].

5.3 Problèmes généraux

Les services de liste d'URI PEUVENT avoir des politiques qui limitent le nombre des URI dans les listes qu'ils acceptent, car une très longue liste pourrait être utilisée dans une attaque de déni de service pour faire peser une lourde charge sur le service de liste d'URI en envoyant un grand nombre de demandes SIP.

Un service de liste d'URI génère un ensemble de demandes provenant d'une liste d'URI. Le paragraphe 19.1.5 de la [RFC3261] fournit des recommandations qui doivent être prises en considération lors de la formation d'une demande provenant d'un URI. Naturellement, ces recommandations s'appliquent à tous les services de liste d'URI SIP.

L'exigence générale de GEN 4, qui déclare que les services de liste d'URI doivent authentifier leurs clients, et les règles précédentes s'appliquent aux services de liste d'URI en général. De plus, les spécifications qui traitent des méthodes individuelles DOIVENT décrire les questions de sécurité relatives à chaque méthode particulière.

6. Considérations relatives à l'IANA

Le présent document définit un nouveau type de disposition de champ d'en-tête Content-Disposition (recipient-list) au paragraphe 4.1. Cette valeur a été enregistrée dans le registre IANA des valeurs et paramètres de disposition de contenu de messagerie avec la description suivante :

recipient-list : le corps inclut une liste des URI auxquels les services de liste d'URI sont à appliquer.

7. Remerciements

Duncan Mills et Miguel A. Garcia-Martin ont soutenu l'idée de 1 à n demandes MESSAGE. Jon Peterson, Dean Willis, et Jonathan Rosenberg ont fourni d'utiles commentaires.

8. Références

8.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2183] R. Troost, S. Dorner, K. Moore, éd., "Communication des informations de présentation dans les messages Internet : le champ d'en-tête Contenu-disposition", août 1997. (*MàJ par* RFC2184, RFC2231) *(P.S.)*

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760)

[RFC5360] J. Rosenberg et autres, "Cadre des communications fondées sur le consentement dans le protocole d'initialisation de session (SIP)", octobre 2008. *(P.S. ; MàJ par* RFC8217)

8.2 Références pour information

[RFC4453] J. Rosenberg et autres, "Exigences pour les communications fondées sur le consentement dans le protocole d'initialisation de session (SIP)", avril 2006. *(Information)*

[RFC4575] J. Rosenberg et autres, "Paquetage d'événement du protocole d'initialisation de session (SIP) pour l'état

Conference", août 2006. *(P.S.)*

[RFC4662] A. B. Roach et autres, "Extension de notification d'événement du protocole d'initialisation de session (SIP) pour les listes de ressources", août 2006. *(P.S.)*

[RFC4825] J. Rosenberg, "Protocole d'accès de configuration (XCAP) du langage de balisage extensible (XML)", mai 2007. *(P.S.)*

[RFC5364] M. Garcia-Martin, G. Camarillo, "Extension de format du langage de balisage extensible (XML) pour la représentation des attributs de contrôle de copie dans les listes de ressources", octobre 2008. *(P.S.)*

[RFC5365] M. Garcia-Martin, G. Camarillo, "Demandes MESSAGE à destinataires multiples dans le protocole d'initialisation de session (SIP)", octobre 2008. *(P.S.)*

[RFC5366] G. Camarillo, A. Johnston, "Établissement de conférence en utilisant des listes contenues dans des demandes dans le protocole d'initialisation de session (SIP)", octobre 2008. *(P.S.)*

[RFC5367] G. Camarillo et autres, "Abonnements aux listes de ressources contenues dans les demandes dans le protocole d'initialisation de session (SIP)", octobre 2008. (*MàJ* RFC3265) *(P.S.)*

Adresse des auteurs

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland
mél : Gonzalo.Camarillo@ericsson.com

Adam Roach
Tekelec
17210 Campbell Rd Ste 250
Dallas, TX 75252
USA
mél : Adam.Roach@tekelec.com

Déclaration complète de droits de reproduction