

Groupe de travail Réseau
Request for Comments : 3097
RFCmise à jour : 2747
Catégorie : En cours de normalisation

R. Braden, ISI
L. Zhang, UCLA
Avril 2001
Traduction Claude Brière de L'Isle

Authentification cryptographique de RSVP – Mise à jour de la valeur de type de message

Statut de ce mémoire

Ce document spécifie un protocole de suivi des normes Internet pour la communauté Internet, et nécessite des discussions et suggestions pour son amélioration. Veuillez vous référer à l'édition courante des "Normes officielles des protocoles de l'Internet" (STD 1) pour l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Copyright

Copyright (C) The Internet Society (2001). Tous droits réservés.

Résumé

Le présent mémoire résout une duplication dans l'allocation des types de messages RSVP, en changeant les types de message alloués par la [RFC2747] aux messages de réponse de défi et d'intégrité.

1. Introduction

La [RFC2747] ("Authentification cryptographique de RSVP") alloue le type de message RSVP 12 à un message Réponse d'intégrité, alors que la [RFC2961] ("Extensions de réduction de redondance de rafraîchissement pour RSVP") alloue la même valeur à un message Faisceau. Le présent mémoire résout le conflit sur le type de message RSVP 12 en allouant une valeur différente au type de message du message Réponse d'intégrité dans la [RFC2747]. On pense que le protocole défini par la RFC2961 est entré en utilisation sur le terrain avant la publication de la RFC et avant que le type de message en conflit ne soit remarqué, et il peut être plus facile d'installer un nouveau logiciel dans des environnements qui ont déployé l'objet Intégrité que dans ceux qui ont déployé l'extension réduction de rafraîchissement.

Pour simplifier de possibles problèmes d'interopérabilité causés par ce changement, on alloue aussi une nouvelle valeur au type de message du message Défi de la [RFC2747], auquel le message Réponse d'intégrité se rapporte.

2. Modification

Les types de message définis dans l'extension d'intégrité RSVP Intégrité [RFC2747] doivent être changés comme suit :

- o Le message Défi a le type de message 25.
- o Le message Réponse d'intégrité a le type de message 25+1.

3. Compatibilité

Deux nœuds communicants dont les mises en œuvre d'Intégrité sont conformes à la présente modification vont interopérer, en utilisant le type de message 12 pour les messages Faisceau et les types de message 25 et 26 pour la prise de contact Intégrité. Une mise en œuvre non conforme de l'extension Intégrité ne va pas interopérer avec une mise en œuvre conforme (bien que deux mises en œuvre non conformes puissent interopérer comme auparavant).

Il n'y a aucune possibilité qu'une prise de contact d'intégrité réussisse accidentellement à cause de ce changement, car les deux côtés de la prise de contact utilisent les nouveaux numéros ou les vieux numéros. De plus, le message Réponse d'intégrité comporte un mouchard de 32 bits qui doit correspondre à un mouchard dans le message Défi, autrement, le défi va échouer. Finalement, une mise en œuvre non conforme ne devrait jamais recevoir un message Faisceau qu'elle interpréterait comme un message Réponse d'intégrité, car la [RFC2961] exige que les messages Faisceau ne soient envoyés qu'à un nœud qui a la capacité Faisceau.

4. Références

[RFC2747] F. Baker, B. Lindell, M. Talwar, "[Authentification cryptographique RSVP](#)", janvier 2000. (MàJ par [RFC3097](#)) (P.S.)

[RFC2961] L. Berger et autres, "Extensions de [réduction de redondance de rafraîchissement](#) pour RSVP", avril 2001. (MàJ par [RFC5063](#)) (P.S.)

Considérations sur la sécurité

Aucune nouvelle considération de sécurité n'est introduite au delà de celles de la [RFC2747] elle-même et des questions de compatibilité ci-dessus.

Adresse des auteurs

Bob Braden
USC Information Sciences Institute
4676 Admiralty Way
Marina del Rey, CA 90292
USA
téléphone : (310) 822-1511
mél : Braden@ISI.EDU

Lixia Zhang
UCLA Computer Science Department
4531G Boelter Hall
Los Angeles, CA 90095-1596
USA
téléphone : 310-825-2695
mél : lixia@cs.ucla.edu

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2000). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de droits de reproduction définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.