Groupe de travail Réseau
Request for Comments : 2480
Catégorie : En cours de normalisation

N. Freed, Innosoft International, Inc.
janvier 1999
Traduction Claude Brière de L'Isle

Les routeurs et les multiparties de sécurité MIME

Statut de ce mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright
Copyright (C) The Internet Society (2003). Tous droits réservés

1. Résumé

Le présent document examine les problèmes associés à l'utilisation des multiparties de sécurité MIME et des passerelles avec des environnements non MIME. Un ensemble d'exigences est défini pour le comportement des passerelles qui fournit les facilités nécessaires pour s'accommoder de façon appropriée du transfert des multiparties de sécurité à travers les passerelles.

2. Notation des exigences

Le présent document utilise occasionnellement des termes qui apparaissent en lettres majuscules. Lorsque les termes "DOIT", "NE DOIT PAS", "DEVRAIT", "NE DEVRAIT PAS", et "PEUT" apparaissent en majuscules, ils sont utilisée pour indiquer des exigences particulières de la présente spécification. Un exposé de la signification des termes "DOIT", "DEVRAIT", et "PEUT" figure dans la [RFC1123] ; les termes "NE DOIT PAS" et "NE DEVRAIT PAS" sont les extensions logiques de cet usage.

3. Le problème

Les multiparties de sécurité [RFC1847] fournissent un moyen efficace d'ajouter des service d'intégrité et de confidentialité aux protocoles qui emploient des objets MIME [RFC2045], [RFC2046]. Des difficultés surviennent cependant dans des environnements hétérogènes qui impliquent des passerelles avec des environnements qui ne prennent pas en charge MIME.

Précisément :

(1) Les services de sécurité doivent être appliqués aux objets MIME dans leur totalité. Manquer à le faire peut conduire à une exposition à des risques pour la sécurité.

Par exemple, une signature qui couvre seulement les données d'objet et non les étiquettes MIME des objets permettrait à quelqu'un d'altérer les étiquettes d'une façon indétectable. De même, manquer à chiffrer les informations d'étiquette MIME expose les informations sur le contenu et pourrait faciliter l'analyse du trafic.

Les objets MIME composites (par exemple, multipart/mixed, message/rfc822) doivent aussi être sécurisés comme un tout. Là encore, manquer à le faire peut faciliter l'altération, révéler sans nécessité des informations importantes, ou les deux.

(2) Les passerelles qui ont affaire à des objets MIME doivent être capables de les convertir en formats non MIME.

Par exemple, les passerelles ont souvent à transformer les informations d'étiquetage MIME en d'autres formes. Les informations de type MIME peuvent finir par être exprimées comme une extension de fichier ou comme un OID.

Les passerelles doivent aussi prendre à part les objets composites MIME dans leurs parties composantes, en convertissant l'ensemble de parties résultant en la forme quelle qu'elle soit qu'utilisent les environnements non MIME pour les objets composites. Manquer à le faire rend les objets inutilisables dans tout environnement qui ne prend pas

MIME en charge. Dans de nombreux cas, cela signifie aussi que les structures MIME multi niveaux doivent être converties en une liste séquentielle de parties.

(3) Les services de sécurité doivent être déployés de bout en bout. Manquer à le faire peut, là encore, conduire à une exposition de la sécurité.

Un service d'intégrité déployé à un autre endroit que le point d'extrémité de la connexion signifie qu'il existe une région, entre le point où le service d'intégrité est appliqué et le point d'extrémité réel, où l'altération de l'objet est possible. Un service de confidentialité déployé ailleurs qu'au point d'extrémité d'une connexion signifie qu'il existe une région où l'objet est transféré en clair. Et pire, les clé privées réparties sont généralement nécessaires chaque fois que quelqu'un d'autre que le générateur applique un service d'intégrité ou que quelqu'un d'autre que le receveur supprime un service de confidentialité, ce qui à son tour peut rendre possible le vol des informations de clé privée.

Tous ces problèmes peuvent bien sûr être réglés. Par exemple, il est possible d'utiliser plusieurs services de sécurité qui se chevauchent pour s'assurer qu'aucune exposition n'existe même si il n'y a pas en soi de sécurité de bout en bout. Et les clés peuvent être distribuées de façon sûre. Cependant, de telles conceptions tendent à être assez complexes, et la complexité dans un système de sécurité est très déconseillée.

Les trois exigences précédentes sont fondamentalement en conflit: Il est possible de satisfaire deux d'entre elles ensemble, mais pas toutes les trois à la fois.

En fait, le conflit est même pire qu'il n'y paraît à première vue. Dans la plupart de ces situations, une sorte de compromis est possible qui, bien que ne satisfaisant complètement aucune des exigences, optimise une sorte de moyenne de toutes les exigences. Une telle solution n'existe cependant pas dans tous ces cas, parce que dans la réalité de nombreuses situations existent où une de ces exigences doit absolument être satisfaite.

4. Résolution du problème

Comme le problème décrit précédemment ne permet pas une solution unique, la seule approche viable est d'exiger que les passerelles fournissent plusieurs solutions. En particulier, les passerelles

(1) DOIVENT fournir la capacité de tunneler les objets multiparties/signés et multiparties/chiffrés comme des entités monolithiques si il y a la plus petite chance qu'existent des capacités MIME sur le côté non MIME de la passerelle. Aucun changement de contenu de l'objet multiparties n'est permis, même lorsque le contenu est lui-même un objet composite MIME.

Cette option doit être fournie afin que les entités derrière la passerelle qui sont capables de traiter les multiparties de sécurité et leur contenu MIME fonctionnent correctement. Comme mentionné précédemment, il existe des situations où les exigences de sécurité de l'application sont absolues et doivent être respectées, même lorsque leur satisfaction pose des problèmes aux autres agents.

Des exceptions ne sont permises que lorsque il n'y a aucune possibilité de prise en charge de MIME sur un côté de la passerelle. Par exemple, une passerelle avec un système de messagerie vocale peut n'avoir aucun moyen utile de représenter un objet MIME signé.

(2) DOIVENT fournir la capacité de prendre à part des objets multiparties/signés, exposant le contenu (et dans le traitement détruisant la signature). Lorsque cette approche est choisie, les passerelles NE DEVRAIENT PAS retirer la signature. Elles DEVRAIENT plutôt garder la signature intacte et y ajouter une note qui sera probablement invalide pour vérifier le contenu du message, mais quand même contenir des informations précieuses sur l'envoyeur.

Cette option doit être fournie afin que les entités derrière la passerelle qui sont incapables de traiter MIME fonctionnent de façon appropriée.

(3) DEVRAIT fournir la capacité de choisir entre les des précédentes options usager par usager.

(4) PEUVENT fournir la capacité de vérifier les signatures et de déchiffrer le contenu chiffré. Une telle facilité NE DOIT PAS être activée par défaut ; l'exposition potentielle de la sécurité impliquée doit être évaluée avant qu'une telle capacité puisse être utilisée.

(5) PEUVENT fournir la capacité de signer et/ou chiffrer le matériel passant du côté non MIME au côté MIME de la passerelle. Là encore, de telles facilités NE DOIVENT PAS être activées pas défaut ; l'exposition potentielle de la

sécurité impliquée dans le transfert de contenu non sécurisé au sein du domaine d'application derrière la passerelle doit être évalué avant qu'une telle capacité puisse être utilisée.

Une passerelle qui se conforme aux exigences ci-dessus est considérée comme étant conforme aux multiparties de sécurité.

5. Considérations sur la sécurité

Le présent document est tout entier sur la sécurité.

6. Références

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la RFC5322*)

[RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – Application et prise en charge", STD 3, octobre 1989.

[RFC1847] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Sécurité multiparties pour MIME : multipartie/signée et multipartie/chiffrée", octobre 1995. *(P.S.)*

[RFC2045] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 1 : Format des corps de message Internet", novembre 1996. *(D. S., MàJ par 2184, 2231, 5335.)*

[RFC2046] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 2 : Types de support", novembre 1996. *(D. S., MàJ par 2646, 3798, 5147, 6657.)*

[RFC2049] N. Freed, N. Borenstein, "Extensions multi-objets de la messagerie Internet (MIME) Partie cinq : critères de conformité et exemples", novembre 1996. *(Remplace RFC1521, RFC1522, RFC1590) (D.S.)*

7. Adresse de l'auteur

Ned Freed
Innosoft International, Inc.
1050 Lakes Drive
West Covina, CA 91790
USA
téléphone : +1 626 919 3600
Fax: +1 626 919 3614
mél : ned.freed@innosoft.com

8. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (1999). 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.