Groupe de travail Réseau
Request for Comments : 3118
Catégorie : En cours de normalisation

R. Droms, éditeur, Cisco Systems
W. Arbaugh, éditeur, University of Maryland
juin 2001
Traduction Claude Brière de L'Isle

Authentification pour les messages DHCP

Résumé
Le présent document définit une nouvelle option du protocole de configuration dynamique d'hôte (DHCP) par laquelle des tickets d'autorisation peuvent être facilement générés et de nouveaux hôtes rattachés avec l'autorisation appropriée peuvent être automatiquement configurés à partir d'un serveur DHCP authentifié. DHCP fournit un cadre pour passer des informations de configuration aux hôtes sur un réseau TCP/IP. Dans certaines situations, les administrateurs de réseau peuvent souhaiter restreindre l'allocation des adresses aux hôtes autorisés. De plus, certains administrateurs de réseau peuvent souhaiter pourvoir à l'authentification des sources et des contenus des messages DHCP.

1. Introduction

DHCP [RFC2131] transporte des paramètres de configuration de la pile de protocoles depuis des serveurs administrés centralement jusqu'à des hôtes TCP/IP. Parmi ces paramètres, il y a une adresse IP. Les serveurs DHCP peuvent être configurés pour allouer de façon dynamique les adresses à partir d'un réservoir d'adresses, éliminant une étape manuelle dans la configuration des hôtes TCP/IP.

Certains administrateurs de réseau peuvent souhaiter fournir l'authentification de la source et du contenu des messages DHCP. Par exemple, les clients peuvent subir des attaques de déni de service par l'utilisation de serveurs DHCP vicieux, ou peuvent être simplement mal configurés du fait de serveurs DHCP involontairement erronés. Les administrateurs de réseau peuvent souhaiter restreindre l'allocation des adresses aux hôtes autorisés pour éviter des attaques de déni de service dans des environnements "hostiles" où le support réseau n'est pas physiquement sécurisé, comme les réseaux sans fils ou les halls de résidences universitaires.

Le présent document définit une technique qui peut fournir l'authentification aux deux entités et l'authentification du message. Le protocole actuel combine le mécanisme original d'authentification de Schiller-Huitema-Droms défini dans un travail en cours antérieur avec la proposition "d'authentification retardée" développée par Bill Arbaugh.

1.1 Modèle des menaces qui pèsent sur DHCP

La menace contre DHCP est par nature une attaque de l'intérieur (en supposant une configuration appropriée du réseau où les accès BOOTP sont bloqués sur les passerelles du périmètre de l'entreprise). Sans considération de la configuration des passerelles, le potentiel d'attaques par l'intérieur et l'extérieur est cependant le même.

L'attaque spécifique d'un client DHCP est la possibilité d'établir un serveur "félon" avec l'intention de fournir des informations de configuration incorrectes au client. Les motivations d'une telle action peuvent être d'établir un attaque "par interposition" ou ce peut être pour une attaque de "déni de service".

Il y a une autre menace pour les clients DHCP de la part de serveurs DHCP configurés par erreur, ou qui répondent accidentellement aux demandes des clients DHCP, avec des paramètres de configuration involontairement incorrects.

La menace spécifique pour un serveur DHCP est un client invalide qui se déguise en client valide. La raison de cette action peut être le "vol de service", ou de circonvenir l'analyse pour diverses raisons malveillantes.

La menace commune au client et au serveur est l'attaque de "déni de service" (DoS) sur une ressource. Ces attaques impliquent normalement l'épuisement des adresses valides, ou l'épuisement de la CPU ou de la bande passante du réseau, et sont présentes chaque fois qu'il y a un partage de ressource. En pratique, c'est la redondance qui atténue le mieux les attaques de DoS.

1.2 Objectifs

Ces objectifs sont ceux qui ont été utilisés pour le développement du protocole d'authentification, énumérés par ordre d'importance :

1. Traiter les menaces présentées au paragraphe 1.1.
2. Éviter de changer le protocole actuel.
3. Limiter les états requis par le serveur.
4. Limiter la complexité (la complexité nourrit les erreurs de conception et de mise en œuvre).

1.3 Exigences de terminologie

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

1.4 Terminologie DHCP

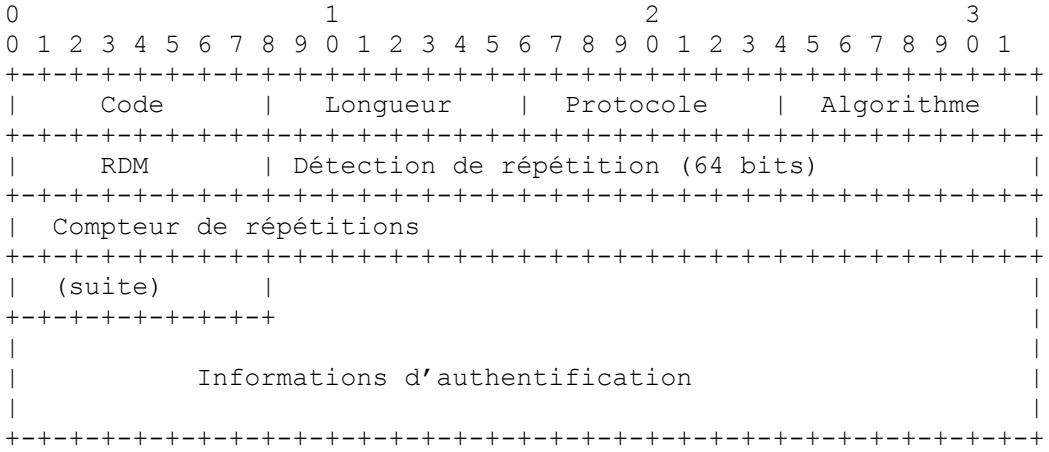
Le présent document utilise les termes suivants :

o "client DHCP"
Un client DHCP ou "client" est un hôte Internet qui utilise DHCP pour obtenir des paramètres de configuration tels que des adresses réseau.

o "serveur DHCP"
Un serveur DHCP ou "serveur" est un hôte Internet qui retourne des paramètres de configuration aux clients DHCP.

2. Format de l'option authentification

Le diagramme qui suit définit le format de l'option d'authentification DHCP :



Le code pour l'option d'authentification est 90, et le champ Longueur contient les champs Longueur du protocole, RDM, Algorithme, Détection de répétition et le champ Informations d'authentifications, en octets.

Le champ Protocole définit la technique particulière utilisée pour l'authentification dans l'option. De nouveaux protocoles sont définis comme décrit à la Section 6.

Le champ Algorithme définit l'algorithme spécifique au sein de la technique identifiée par le champ Protocole.

Le champ Détection de répétition est selon la RDM, et le champ Informations d'authentification selon le protocole utilisé.

Le champ Méthode de détection de répétition (RDM, *Replay Detection Method*) détermine le type de détection de répétition utilisée dans le champ Détection de répétition.

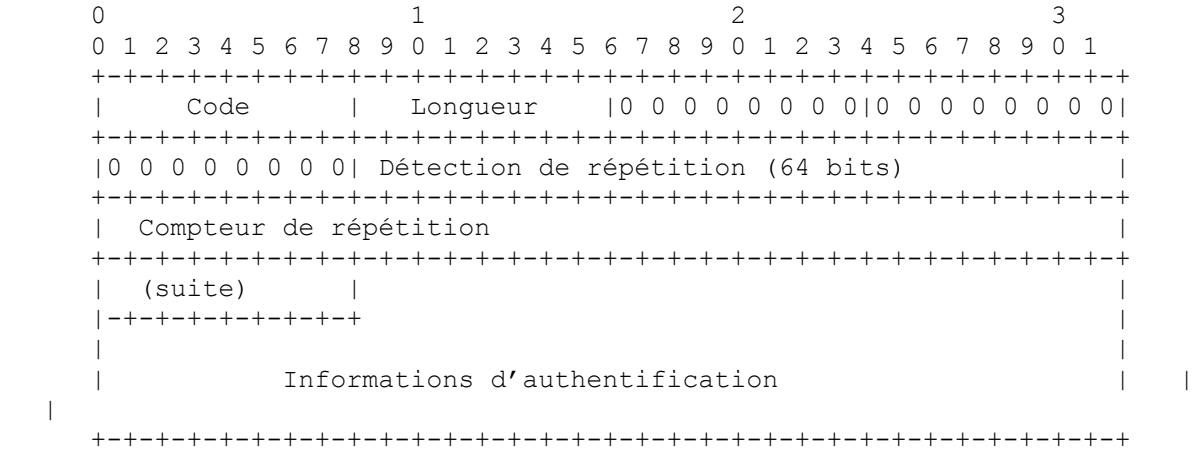
Si le champ RDM contient 0x00, le champ Détection de répétition DOIT être réglé à la valeur d'un compteur à accroissement monotone. Utiliser une valeur de compteur telle que l'heure courante (par exemple, un horodatage au format NTP [RFC1305]) peut réduire le danger des attaques en répétition. Cette méthode DOIT être prise en charge par tous les protocoles.

3. Interaction avec les agents de relais

Parce que un agent de relais DHCP peut altérer les valeurs des champs "giaddr" et "hops" dans le message DHCP, le contenu de ces deux champs DOIT être réglé à zéro pour le calcul de toute fonction de hachage sur l'en-tête de message. De plus, un agent de relais peut ajouter l'option DHCP 82, Informations d'agent de relais [RFC3046] comme dernière option dans un message aux serveurs. Si un serveur trouve l'option 82 incluse dans un message reçu, le serveur DOIT calculer toute fonction de hachage comme si l'option N'ÉTAIT PAS incluse dans le message sans changer l'ordre des options. Chaque fois que le serveur renvoie l'option 82 à un agent de relais, le serveur DOIT ne pas inclure l'option dans le calcul de toute fonction de hachage sur le message.

4. Jeton de configuration

Si le champ Protocole est 0, le champ Informations d'authentification contient un simple jeton de configuration :



Le jeton de configuration est une valeur opaque, non codée, connue de l'envoyeur et du receveur. L'envoyeur insère le jeton de configuration dans le message DHCP et le receveur confronte le jeton du message au jeton partagé. Si l'option Configuration est présente et si le jeton du message ne correspond pas au jeton partagé, le receveur DOIT éliminer le message.

Le jeton de configuration peut être utilisé pour passer un jeton de configuration en clair et fournir seulement une faible authentification d'entité et pas d'authentification de message. Ce protocole n'est utile que pour une protection rudimentaire contre des mises en œuvre de serveur DHCP accidentellement fautives.

Discussion :
L'intention est ici de passer un jeton constant, non calculé comme un mot de passe en clair. D'autres types d'authentification d'entité utilisant des jetons calculés tels que des tickets Kerberos ou des mots de passe à utilisation unique seront définis dans des protocoles distincts.

5. Authentification retardée

Si le champ Protocole est 1, le message utilise le mécanisme "authentification retardée". Dans l'authentification retardée, le client demande l'authentification dans son message DHCPDISCOVER et le serveur répond avec un message DHCPOFFER qui comporte des informations d'authentification. Ces informations d'authentification contiennent une valeur de nom occasionnel générée par la source comme un code d'authentification de message (MAC) pour fournir l'authentification de message et l'authentification d'entité.

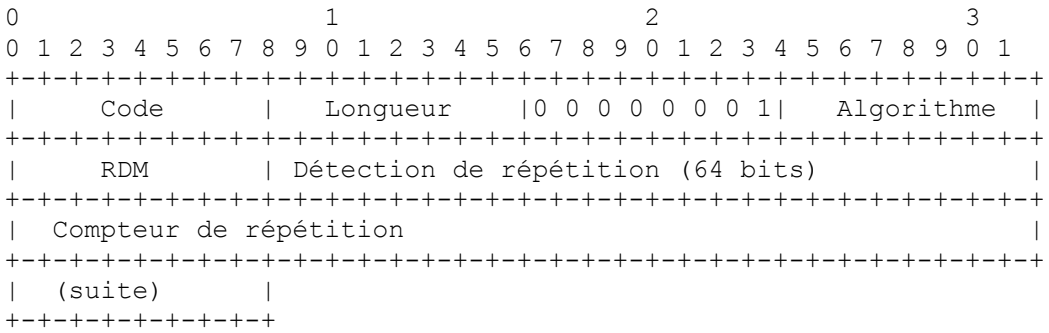
Le présent document définit l'utilisation d'une technique particulière fondés sur le protocole HMAC [RFC2104] en utilisant le hachage MD5 [RFC1321].

5.1 Questions de gestion

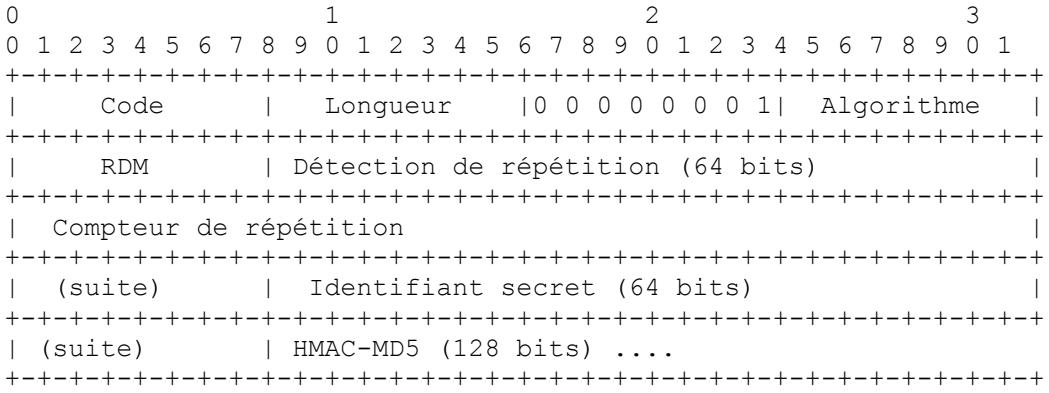
Le protocole "d'authentification retardée" n'essaye pas de régler des situations où un client peut circuler d'un domaine administratif à l'autre, c'est-à-dire, l'itinérance interdomaines. Le présent protocole se concentre sur la résolution du problème intradomaine où l'échange hors bande d'un secret partagé est faisable.

5.2 Format

Le format de la demande d'authentification dans un message DHCPDISCOVER ou DHCPINFORM pour l'authentification retardée est :



Le format des informations d'authentification dans un message DHCPOFFER, DHCPREQUEST ou DHCPACK pour l'authentification retardée est :



Les définitions suivantes seront utilisées dans la description des informations d'authentification pour l'authentification retardée, algorithme 1 :

Détection de répétition	comme défini par le champ RDM
K	valeur secrète partagée entre la source et la destination du message ; chaque secret a un identifiant univoque (ID de secret)
ID secret	identifiant univoque pour la valeur secrète utilisée pour générer le MAC pour ce message
HMAC-MD5	fonction de génération du MAC [RFC2104], [RFC1321].

L'envoyeur calcule le MAC en utilisant l'algorithme de génération HMAC [RFC2104] et la fonction de hachage MD5 [RFC1321]. Le message DHCP entier (excepté comme noté ci-dessous) y compris l'en-tête de message DHCP et le champ Options, est utilisé comme entrée à la fonction de calcul HMAC-MD5. Le champ "ID de secret" DOIT être réglé sur l'identifiant du secret utilisé pour générer le MAC.

Discussion :
L'algorithme 1 spécifie l'utilisation de HMAC-MD5. L'utilisation d'une technique différente, telle que HMAC-SHA, sera spécifiée dans un autre protocole.

L'authentification retardée exige une clé secrète partagée pour chaque client sur chaque serveur DHCP avec lequel ce client peut souhaiter utiliser le protocole DHCP. Chaque clé secrète a un identifiant univoque qui peut être utilisé par un receveur pour déterminer quel secret a été utilisé pour générer le MAC dans le message DHCP. Donc, l'authentification retardée peut ne pas bien s'adapter dans une architecture dans laquelle un client DHCP se connecte à plusieurs domaines administratifs.

5.3 Validation de message

Pour valider un message entrant, le receveur vérifie d'abord que la valeur dans le champ Détection de répétition est acceptable selon la méthode de détection de répétition spécifiée par le champ RDM. Ensuite, le receveur calcule le MAC comme décrit dans la [RFC2104]. Le receveur DOIT régler le champ "MAC" de l'option d'authentification tout à 0 pour le calcul du MAC, et parce que un agent de relais DHCP peut altérer les valeurs des champs "giaddr" et "hops" dans le message DHCP, le contenu de ces deux champs DOIT aussi être réglé à zéro pour le calcul du MAC. Si le MAC calculé par le receveur ne correspond pas au MAC contenu dans l'option d'authentification, le receveur DOIT éliminer le message DHCP.

La Section 3 donne des informations supplémentaires sur le traitement des messages qui incluent l'option 82 (Agents de relais).

5.4 Utilisation des clés

Chaque client DHCP a une clé, K. Le client utilise sa clé pour coder tous les messages qu'il envoie au serveur et pour authentifier et vérifier tous les messages qu'il reçoit du serveur. La clé du client DEVRAIT être initialement distribuée au client par un mécanisme hors bande, et DEVRAIT être mémorisée localement chez le client pour être utilisée dans tous les messages DHCP authentifiés. Une fois que le client a reçu sa clé, il DEVRAIT utiliser cette clé pour toutes les transactions même si la configuration du client change; par exemple, si le client se voit allouer une nouvelle adresse réseau.

Chaque serveur DHCP DOIT connaître, ou être capable d'obtenir d'une manière sûre, les clés pour tous les clients autorisés. Si tous les clients utilisent la même clé, ils peuvent effectuer l'authentification à la fois de message et d'entité pour tous les messages reçus des serveurs. Cependant, le partage des clés est fortement déconseillé car il permet à des clients non autorisés de se faire passer pour des clients autorisés en obtenant une copie de la clé partagée. Pour authentifier l'identité des clients individuels, chaque client DOIT être configuré avec une clé unique. L'Appendice A décrit une technique de gestion des clés.

5.5 Considérations sur le client

Cette section décrit le comportement d'un client DHCP qui utilise l'authentification retardée.

5.5.1 État INIT

Dans l'état INIT, le client utilise l'authentification retardée comme suit :

1. Le client DOIT inclure l'option Demande d'authentification dans son message DHCPDISCOVER avec une option Identifiant de client [RFC2132] pour s'identifier de façon univoque auprès du serveur.

2. Le client DOIT effectuer l'essai de validation décrit au paragraphe 5.3 sur tout message DHCPOFFER qui comporte des informations d'authentification. Si un ou plusieurs messages DHCPOFFER réussissent l'essai de validation, le client choisit une des configurations offertes.

Le comportement du client, si aucun message DHCPOFFER ne comporte d'informations d'authentification ou ne réussit l'essai de validation, est contrôlé par la politique locale chez le client. Conformément à la politique du client, celui-ci PEUT choisir de répondre au message DHCPOFFER qui n'a pas été authentifié.

La décision de régler la politique locale à accepter les messages non authentifiés devrait être prise avec prudence. Accepter un message DHCPOFFER non authentifié peut rendre le client vulnérable à des mystifications et autres attaques. Si les utilisateurs locaux ne sont pas explicitement informés que le client a accepté un message DHCPOFFER non authentifié, les utilisateurs peuvent à tort supposer que le client a reçu une adresse authentifiée et qu'il n'est pas sujet à des attaques contre DHCP au travers de messages non authentifiés.

Un client DOIT être configurable pour décliner les messages non authentifiés, et DEVRAIT être configuré par défaut à décliner les messages non authentifiés. Un client PEUT choisir de différencier entre les messages DHCPOFFER sans informations d'authentification et les messages DHCPOFFER qui ne réussissent pas l'essai de validation ; par exemple, un client pourrait accepter le premier et éliminer le dernier. Si un client accepte un message non authentifié, le client DEVRAIT informer tous les utilisateurs locaux et DEVRAIT enregistrer l'événement.

3. Le client répond par un message DHCPREQUEST qui DOIT inclure des informations d'authentification codées avec le même secret utilisé par le serveur dans le message DHCPOFFER choisi.

4. Si le client a authentifié le DHCPOFFER qu'il a accepté, il DOIT valider le message DHCPACK provenant du serveur. Le client DOIT éliminer le DHCPACK si le message échoue à la validation et PEUT enregistrer dans le journal l'échec de la validation. Si le DHCPACK échoue à la validation, le client DOIT revenir à l'état INIT et retourner à l'étape 1. Le client PEUT choisir de se souvenir du serveur qui a répondu avec un message DHCPACK qui n'a pas réussi sa validation et éliminer les messages ultérieurs qui proviennent de ce serveur.

Si le client a accepté un message DHCPOFFER qui ne comportait pas d'informations d'authentification ou qui n'a pas réussi l'essai de validation, le client PEUT accepter un message DHCPACK non authentifié du serveur.

5.5.2 État INIT-REBOOT

Dans l'état INIT-REBOOT, le client DOIT utiliser le secret dont il se servait dans son message DHCPREQUEST pour obtenir sa configuration actuelle pour générer les informations d'authentification pour le message DHCPREQUEST. Le client PEUT choisir d'accepter des messages DHCPACK/DHCPNAK non authentifiés si aucun message authentifié n'a été reçu. Le client DOIT traiter la réception (ou l'absence de réception) de tout message DHCPACK/DHCPNAK comme spécifié au paragraphe 3.2 de la [RFC2131].

5.5.3 État RENEWING

Dans l'état RENEWING, le client utilise le secret qu'il a utilisé dans son message initial DHCPREQUEST pour obtenir sa configuration actuelle pour générer les informations d'authentification pour le message DHCPREQUEST. Si le client ne reçoit pas de message DHCPACK ou si aucun message DHCPACK ne réussit la validation, le client se comporte comme si il n'avait pas reçu de message DHCPACK selon le paragraphe 4.4.5 de la spécification DHCP [RFC2131].

5.5.4 État REBINDING

Dans l'état REBINDING, le client utilise le secret qu'il a utilisé dans son message initial DHCPREQUEST pour obtenir sa configuration actuelle pour générer les informations d'authentification pour le message DHCPREQUEST. Si le client ne reçoit pas de message DHCPACK ou si aucun message DHCPACK ne réussit la validation, le client se comporte comme si il n'avait pas reçu de message DHCPACK selon le paragraphe 4.4.5 de la spécification DHCP [RFC2131].

5.5.5 Message DHCPINFORM

Comme le client a déjà des informations de configuration, il peut aussi avoir établi une valeur de secret partagé, K, avec un serveur. Donc, le client DEVRAIT utiliser la demande d'authentification comme dans un message DHCPDISCOVER lorsque il existe une valeur de secret partagé. Le client DOIT traiter tous les messages DHCPACK reçus comme il fait des messages DHCPOFFER ; voir au paragraphe 5.5.1.

5.5.6 Message DHCPRELEASE

Comme le client est déjà dans l'état BOUND, il va avoir une association de sécurité déjà établie avec le serveur. Donc, le client DOIT inclure les informations d'authentification avec le message DHCPRELEASE.

5.6 Considérations sur le serveur

Cette section décrit le comportement d'un serveur en réponse au messages de client en utilisant l'authentification retardée.

5.6.1 Considérations générales

Chaque serveur tient une liste des secrets et identifiants pour les secrets qu'il partage avec les clients et les clients potentiels. Ces information doivent être tenues de telle façon que le serveur puisse :

* Identifier un secret approprié et l'identifiant pour ce secret à utiliser avec un client avec lequel le serveur peut n'avoir pas été en communication auparavant.
* Restituer le secret et l'identifiant utilisés par un client auquel le serveur a fourni précédemment ses informations de configuration.

Chaque serveur DOIT sauvegarder le compteur à partir du message authentifié précédent. Un serveur DOIT éliminer tout message entrant qui échoue à la vérification de détection de répétition comme défini par le procédé RDM d'évitement des attaques en répétition.

Discussion :
Le message DHCPREQUEST authentifié venant d'un client dans l'état INIT-REBOOT ne peut être validé que par des serveurs qui ont utilisé le même secret dans leurs messages DHCPOFFER. Les autres serveurs vont éliminer le message DHCPREQUEST. Donc, seuls les serveurs qui ont utilisé le secret choisi par le client seront capables de déterminer que leur offre d'informations de configuration n'a pas été choisie et que l'adresse réseau offerte peut être remise dans le réservoir d'adresses disponibles du serveur. Les serveurs qui ne peuvent pas valider le message DHCPREQUEST vont finalement retourner leur offre d'adresses réseau à leur réservoir d'adresses disponibles, comme décrit au paragraphe 3.1 de la spécification DHCP, la [RFC2131].

5.6.2 À réception d'un message DHCPDISCOVER

Le serveur choisit un secret pour le client et inclut les informations d'authentification dans le message DHCPOFFER comme spécifié à la section 5, ci-dessus. Le serveur DOIT enregistrer l'identifiant du secret choisi pour le client et utiliser ce même secret pour valider les messages ultérieurs avec le client.

5.6.3 À réception d'un message DHCPREQUEST

Le serveur utilise le secret identifié dans le message et valide le message comme spécifié au paragraphe 5.3. Si le message échoue à la validation ou si le serveur ne connaît pas le secret identifié par le champ "ID de secret", le serveur DOIT éliminer le message et PEUT choisir d'enregistrer l'échec de validation dans son journal d'événements.

Si le message réussit la procédure de validation, le serveur répond comme décrit dans la spécification DHCP. Le serveur DOIT inclure les informations d'authentification générées comme spécifié au paragraphe 5.2.

5.6.4 À réception d'un message DHCPINFORM

Le serveur PEUT choisir d'accepter des messages DHCPINFORM non authentifiés, ou de n'accepter que des messages DHCPINFORM authentifiés sur la base de la politique du site.

Lorsque un client inclut la demande d'authentification dans un message DHCPINFORM, le serveur DOIT répondre par un message DHCPACK authentifié. Si le serveur n'a pas de valeur de secret partagé établie avec l'envoyeur du message DHCPINFORM, le serveur PEUT alors répondre par un message DHCPACK non authentifié, ou un DHCPNAK si le serveur n'accepte pas les clients non authentifiés sur la base de la politique du site, ou le serveur PEUT choisir de ne pas répondre au message DHCPINFORM.

6. Considérations pour l'IANA

La Section 2 définit une nouvelle option DHCP appelée option d'authentification , dont le code d'option est 90.

Le présent document spécifie trois nouveaux espaces de noms associés à l'option Authentification, qui sont à créer et entretenir par l'IANA : Protocole, Algorithme et RDM.

Les valeurs initiales allouées à partir de l'espace de nom Protocole sont 0 (pour le jeton de configuration Protocole de la section 4) et 1 (pour le protocole d'authentification retardée de la section 5). Des valeurs supplémentaires de l'espace de nom Protocole seront allouées par consensus de l'IETF, comme défini dans la [RFC2434].

L'espace de nom Algorithme est spécifique de chaque protocole. C'est-à-dire que chaque protocole a son propre espace de nom d'algorithme. Les lignes directrices pour allouer les valeurs de l'espace de nom d'algorithme pour un protocole particulier devraient être spécifiées avec la définition d'un nouveau protocole.

Pour le protocole de jeton de configuration, le champ Algorithme DOIT être 0. Pour le protocole d'authentification retardée, la valeur de Algorithme 1 est allouée à la fonction génératrice HMAC-MD5 comme défini à la section 5. Des valeurs supplémentaires provenant de l'espace de nom Algorithme pour l'algorithme 1 seront allouées par consensus de l'IETF, comme défini dans la [RFC2434].

La valeur initiale de 0 provenant de l'espace de nom RDM est allouée à l'utilisation d'une valeur à accroissement monotone, comme défini à la section 2. Des valeurs supplémentaires de l'espace de nom RDM seront allouées par consensus de l'IETF, comme défini dans la [RFC2434].

7. Références

[RFC1305] D. Mills, "Protocole de l'heure du réseau, version 3, spécification, mise en œuvre et analyse", STD 12, mars 1992. *(Remplacée par RFC5905)*

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992. *(Information)*

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

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

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(M. à j. par les RFC 3396 et 4361)*

[RFC2132] S. Alexander et R. Droms, "Options DHCP et Extensions de fabricant BOOTP", mars 1997.

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la RFC 5226)*

[RFC3046] M. Patrick, "Option DHCP Information d'agent de relais", janvier 2001.

8. Remerciements

Jeff Schiller et Christian Huitema ont développé la version originale de ce protocole d'authentification à la journée finale d'une session ouverte à tous de la réunion de Dallas de l'IETF en décembre 1995. Un des éditeurs (Droms) a transcrit les notes de cette discussion, qui forme la base du présent document. Les éditeurs remercient Jeff et Christian de leur patience a revoir ce document et ses projets antérieurs.

Le mécanisme de "l'authentification retardée" utilisé à la section 5 est dû à Bill Arbaugh. Le modèle de menaces et les exigences des paragraphes 1.1 et 1.2 viennent de la proposition de protocole de négociation de Bill. Les participants à la réunion intermédiaire du groupe de travail DHC tenue en juin 1998, y compris Peter Ford, Kim Kinnear, Glenn Waters, Rob Stevens, Bill Arbaugh, Baiju Patel, Carl Smith, Thomas Narten, Stewart Kwan, Munil Shah, Olafur Gudmundsson, Robert Watson, Ralph Droms, Mike Dooley, Greg Rabil et Arun Kapur, ont développé le modèle de menace et discuté plusieurs propositions de solutions de remplacement.

Le champ Méthode de détection de répétition est dû à Vipul Gupta.

Nous remercierons chaleureusement Bill Sommerfield de ses contributions.

Merci aussi à John Wilkins, Ran Atkinson, Shawn Mamros et Thomas Narten pour leur révision des premiers projets de ce document.

9. Considérations pour la sécurité

Le présent document décrit les mécanismes d'authentification et de vérification pour DHCP.

9.1 Faiblesses du protocole

Le mécanisme d'authentification de jeton de configuration est vulnérable à l'interception et ne fournit que la protection la plus rudimentaire contre les serveurs DHCP accidentellement mal conformés.

Le mécanisme d'authentification retardée décrit dans le présent document est vulnérable à une attaque de déni de service par l'inondation de messages DHCPDISCOVER, qui ne sont pas authentifiés par ce protocole. Une telle attaque peut submerger l'ordinateur sur lequel fonctionne le serveur DHCP et peut épuiser les adresses disponibles à allouer par le serveur DHCP.

L'authentification retardée peut aussi être vulnérable à une attaque de déni de service par inondation de messages authentifiés, qui peuvent submerger l'ordinateur sur lequel fonctionne le serveur DHCP lors du calcul des clés d'authentification pour les messages entrants.

9.2 Limitations du protocole

L'authentification retardée n'accepte pas l'authentification inter domaine.

Un mécanisme de signature numérique réel tel que RSA, bien qu'actuellement computationnellement infaisable, fournirait une meilleure sécurité.

10. Adresse des éditeurs

Ralph Droms
Cisco Systems
300 Apollo Drive
Chelmsford, MA 01824
téléphone : (978) 244-4733
mél : rdroms@cisco.com

Bill Arbaugh
Department of Computer Science
University of Maryland
A.V. Williams Building
College Park, MD 20742
téléphone : (301) 405-2774
mél : waa@cs.umd.edu

Appendice A Technique de gestion des clés

Pour éviter la gestion centralisée d'une liste de clés aléatoires, on suppose que pour chaque client K est généré à partir de la paire (identifiant de client [RFC2132], adresse de sous-réseau, par exemple, 192.168.1.0) qui doit être unique pour ce client. C'est à dire, K = MAC(MK, id-unique) où MK est une clé secrète maîtresse et MAC est une fonction de clé unidirectionnelle telle que le HMAC-MD5.

Sans connaissance de la clé maîtresse MK, un client non autorisé ne peut pas générer sa propre clé K. Le serveur peut rapidement valider un message entrant provenant d'un nouveau client en régénérant K à partir de l'identifiant de client. Pour les clients connus, le serveur peut choisir de retrouver de façon dynamique le K du client à partir de l'identifiant de client dans le message DHCP, ou il peut choisir de précalculer et mettre en antémémoire tous les K à priori.

En déduisant toutes les clés à partir d'une seule clé maîtresse, le serveur DHCP n'a pas besoin d'accéder à des mots de passe en clair, et peut calculer et vérifier les MAC à clés sans requérir à l'aide d'un serveur d'authentification centralisé.

Pour éviter de compromettre ce système de gestion de clés, les clés maîtresses, MK, NE DOIVENT PAS être mémorisées par les clients. Le client DEVRAIT seulement recevoir sa clé, K. Si MK est compromis, un nouveau MK DEVRAIT être choisi et tous les clients DEVRAIENT recevoir une nouvelle clé individuelle.

Déclaration complète de droits de reproduction

Remerciement

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