Groupe de travail Réseau
Request for Comments : 5090
RFC rendue obsolète : 4590
Catégorie : Sur la vois de la normalisation

Traduction Claude Brière de L'Isle

B. Sterman, Kayote Networks
D. Sadolevsky, SecureOL, Inc.
D. Schwartz, Kayote Networks
D. Williams, Cisco Systems
W. Beck, Deutsche Telekom AG
février 2008

Extension RADIUS pour authentification par résumé

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

Résumé
Le présent document définit une extension au protocole du service d'authentification distante d'utilisateur appelant (RADIUS, *Remote Authentication Dial-In User Service*) pour permettre la prise en charge de l'authentification par résumé, à utiliser avec les protocoles de style HTTP comme le protocole d'initialisation de session (SIP) et HTTP.

Table des matières

1. Introduction

1.1 Motifs

Le mécanisme d'authentification par résumé HTTP, défini dans la [RFC2617], a été ultérieurement adapté pour être utilisé avec SIP [RFC3261]. Du fait des limitations et des faiblesses de l'authentification par résumé (voir la Section 4 de la [RFC2617]) des mécanismes supplémentaires d'authentification et de chiffrement sont définis dans SIP [RFC3261], incluant la sécurité de la couche Transport (TLS, *Transport Layer Security*) [RFC4346] et MIME sécurisé (S/MIME) [RFC3851]. Cependant, la prise en charge de l'authentification par résumé est obligatoire dans les mises en œuvre de SIP, et l'authentification par résumé est la façon préférée pour un agent d'utilisateur SIP de s'authentifier auprès d'un serveur mandataire. L'authentification par résumé est aussi utilisée dans d'autres protocoles.

Pour simplifier l'approvisionnement des utilisateurs, il y a un besoin de prise en charge de ce mécanisme d'authentification dans les protocoles d'authentification, d'autorisation, et de comptabilité (AAA, *Authentication, Authorization, and Accounting*) comme RADIUS [RFC2865] et Diameter [RFC3588].

Le présent document définit une extension au protocole RADIUS pour permettre la prise en charge de l'authentification par résumé à utiliser avec les protocoles SIP, HTTP, et autres de style HTTP qui utilisent cette méthode d'authentification. La prise en charge des mécanismes de résumé comme l'authentification et l'accord de clé (AKA, *Authentication and Key Agreement*) [RFC3310] est aussi incluse. Un document d'accompagnement, la [RFC4740], définit la prise en charge de l'authentification par résumé dans Diameter.

1.2 Terminologie

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

L'utilisation des mots clés d'exigence normative dans le présent document devra s'appliquer uniquement aux mises en œuvre de client RADIUS et de serveur RADIUS qui incluent les caractéristiques décrites dans ce document. Le présent document ne crée aucune exigence normative pour les mises en œuvre existantes.

Protocole de style HTTP : ce terme note tout protocole qui utilise des en-têtes de style HTTP et utilise l'authentification par résumé HTTP comme décrite dans la [RFC2617]. Des exemples sont HTTP et le protocole d'initialisation de session (SIP).

Serveur d'accès réseau (NAS, *Network Access Server*) : le client RADIUS.

Nom occasionnel *(nom occasionnel)* : valeur non prédictible utilisée poue empêcher les attaques en répétition. Le générateur de noms occasionnels peut utiliser des mécanismes cryptographiques pour produire des noms occasionnels qu'il peut reconnaître sans conserver l'état.

Espace de protection : les protocoles de style HTTP diffèrent dans leur définition de l'espace de protection. Pour HTTP, il est défini comme la combinaison du domaine et de l'URI racine canonique de la ressource demandée pour laquelle l'utilisation est autorisée par le serveur RADIUS. Dans le cas de SIP, la chaîne de domaine seule définit l'espace de protection.

Agent d'utilisateur SIP *(SIP UA)* : point d'extrémité Internet qui utilise le protocole d'initialisation de session.

Serveur d'agent d'utilisateur SIP *(SIP UAS)* : entité logique qui génère une réponse à une demande SIP.

1.3 Généralités

HTTP Digest est un protocole de défi-réponse utilisé pour authentifier la demande d'un client pour accéder à une ressource sur un serveur. La Figure 1 montre une seule transaction HTTP Digest.

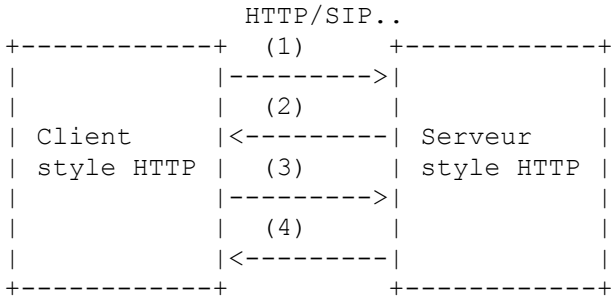


Figure 1 : Opération Digest sans RADIUS

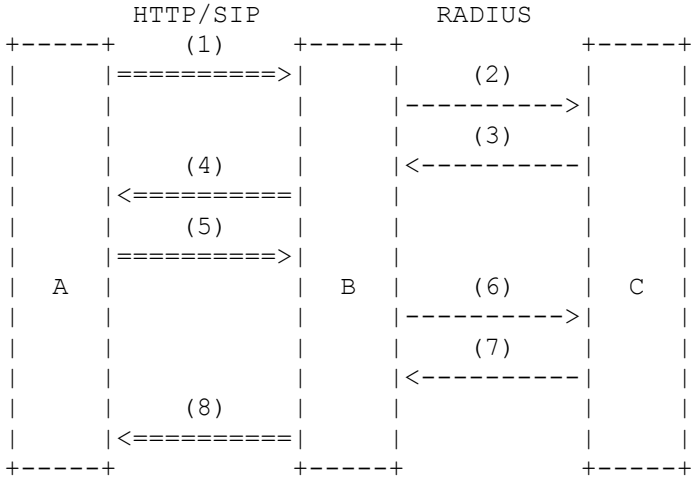
Si le client envoie une demande sans aucun accréditif (1), le serveur va répliquer par une réponse d'erreur (2) contenant un nom occasionnel. Le client crée un résumé cryptographique de parties de la demande, du nom occasionnel reçu du serveur, et d'un secret partagé. Le client retransmet la demande (3) au serveur, mais y inclut maintenant le résumé dans le paquet. Le serveur fait le même calcul de résumé que le client et compare le résultat à celui reçu dans (3). Si les valeurs de résumé sont identiques, le serveur accorde l'accès à la ressource et envoie une réponse positive au client (4). Si les valeurs de résumé diffèrent, le serveur envoie une réponse négative au client (4).

Au lieu de conserver une base de données d'utilisateur locale, le serveur pourrait utiliser RADIUS pour accéder à une base de données d'utilisateurs centralisée. Cependant, RADIUS [RFC2865] n'inclut pas la prise en charge de l'authentification par résumé HTTP. Le client RADIUS ne peut pas utiliser l'attribut Mot de passe d'utilisateur, car il ne reçoit pas de mot de passe du client de style HTTP. Les attributs Défi CHAP et Mot de passe CHAP décrits dans la [RFC1994] ne conviennent pas non plus parce que l'algorithme du protocole d'authentification par dialogue à énigme (CHAP, *Challenge Handshake Authentication Protocol*) n'est pas compatible avec le résumé HTTP.

Le présent document définit de nouveaux attributs qui permettent au serveur RADIUS d'effectuer le calcul de résumé comme défini dans la [RFC2617], fournissant la prise en charge de l'authentification par résumé comme mécanisme d'authentification natif au sein de RADIUS.

Les noms occasionnels requis par l'algorithme de résumé sont générés par le serveur RADIUS. Les générer dans le client RADIUS économiserait un aller-retour, mais introduirait des problèmes de sécurité et de fonctionnement. Certains algorithmes de résumé – par exemple, AKA [RFC3310] – ne fonctionneraient pas.

La Figure 2 décrit un scénario où le serveur de style HTTP délègue l'authentification à un serveur RADIUS. Les entités A et B communiquent avec HTTP ou SIP, alors que les entités B et C communiquent en utilisant RADIUS.



====> HTTP/SIP
----> RADIUS

Figure 2 : Résumé HTTP sur RADIUS

Les entités ont les rôles suivants :
A : client HTTP / UA SIP

B : {serveur HTTP / serveur mandataire HTTP / serveur mandataire SIP/ UAS SIP} agissant aussi comme NAS RADIUS
C : serveur RADIUS

Les messages suivants sont envoyés dans ce scénario :

A envoie à B une demande HTTP/SIP sans en-tête Autorisation (étape 1). B envoie au serveur RADIUS, C (étape 2) un paquet Demande d'accès avec les nouveaux attributs définis, Méthode de résumé et URI de résumé, mais sans attribut Nom occasionnel de résumé. C choisit un nom occasionnel et répond avec un Défi d'accès (étape 3). Ce Défi d'accès contient des attributs Résumé, d'où B prend des valeurs pour construire une réponse HTTP/SIP "Autorisation (mandataire) exigée". B envoie cette réponse à A (étape 4). A renvoie cette demande avec ses accréditifs (étape 5). B envoie un message Demande d'accès à C (étape 6). C vérifie les accréditifs et réplique par un message Accès-accepté ou Accès-rejeté (étape 7). Selon le résultat de C, B traite la demande de A ou la rejette avec une réponse "Autorisation (mandataire) exigée" (étape 8).

2. Description détaillée

2.1 Comportement du client RADIUS

Les attributs décrits dans ce document sont envoyés en clair. Donc, si le client RADIUS devait accepter des connections sécurisées (HTTPS ou SIPS) de la part des clients de style HTTP, il pourrait en résulter que des informations intentionnellement protégées par les clients de style HTTP soient envoyées en clair durant l'échange RADIUS.

2.1.1 Choix d'accréditifs

À réception d'un message de demande de style HTTP, le client RADIUS vérifie si il est autorisé à authentifier la demande. Lorsque une demande de style HTTP traverse plusieurs mandataires, et que chacun des mandataires demande à authentifier le client de style HTTP, la demande au serveur de style HTTP peut contenir plusieurs jeux d'accréditifs.

Le client RADIUS peut utiliser la directive domaine dans HTTP pour déterminer quels accréditifs sont applicables. Lorsque aucun des domaines n'est intéressant, le client RADIUS DOIT se comporter comme si aucun accréditif pertinent n'avait été envoyé. Dans toutes les situations, le client RADIUS DOIT envoyer zéro ou exactement un accréditif au serveur RADIUS. Le client RADIUS DOIT choisir l'accréditif de l'en-tête Autorisation (mandataire) si la directive de domaine correspond à son domaine configuré en local.

2.1.2 Construction d'une demande d'accès

Si un en-tête Autorisation (mandataire) correspondant est présent et contient les informations de résumé HTTP, le client RADIUS vérifie le paramètre Nom occasionnel.

Si le client RADIUS reconnaît le nom occasionnel, il prend les directives d'en-tête et les met dans un paquet Demande d'accès RADIUS. Il met la directive de réponse dans un attribut Réponse de résumé et les directives Domaine, Nom occasionnel, uri de résumé, qop, algorithme, cnonce, nc, nom d'utilisateur, et opaque dans les attributs respectifs Domaine de résumé, Nom occasionnel de résumé, URI de résumé, Qop de résumé, Algorithme de résumé, Cnonce de résumé, Compte de noms occasionnels de résumé, Nom d'utilisateur de résumé, et Digest-Opaque. Le client RADIUS met la méthode de demande dans l'attribut Méthode de résumé.

Du fait des exigences syntaxiques de HTTP, les chaînes entre guillemets trouvées dans les directives Résumé HTTP peuvent contenir des caractères guillemets et barre oblique inverse échappés. Lors de la traduction de ces directives en attributs RADIUS, le client RADIUS retire seulement les caractères guillemets de tête et de queue qui entourent la valeur de la directive, il ne retire pas les échappements de quoi que ce soit d'autre dans la chaîne. Voir un exemple à la Section 3.

Si la valeur de la directive Qualité de protection (qop) est "uth-int", le client RADIUS calcule H(corps d'entité) comme décrit dans la [RFC2617], paragraphe 3.2.1, et met le résultat dans un attribut Hachage de corps d'entité de résumé *(hachage de corps d'entité de résumé)*.

Le client RADIUS ajoute un attribut Authentifiant de message, défini dans la [RFC3579], et envoie le paquet Demande d'accès au serveur RADIUS.

Le serveur RADIUS traite le paquet et répond avec un Accès-accepté ou un Accès-rejeté.

2.1.3 Construction d'un en-tête Informations d'authentification

Après avoir reçu un Accès-accepté du serveur RADIUS, le client RADIUS construit un en-tête Informations d'authentification :

- Si le paquet Accès-accepté contient un attribut Auth de réponse de résumé, le client RADIUS vérifie l'attribut Qop de résumé :
  - Si la valeur de l'attribut Qop de résumé est "auth" ou n'est pas spécifiée, le client RADIUS met le contenu de l'attribut Auth de réponse de résumé dans la directive rspauth de l'en-tête Informations d'authentification de la réponse de style HTTP.
  - Si la valeur de l'attribut Qop de résumé est "auth-int", le client RADIUS ignore le paquet Accès-accepté et se comporte comme si il avait reçu un paquet Accès-rejeté (Auth de réponse de résumé ne peut être correct car le serveur RADIUS ne connaît pas le contenu du corps de la réponse de style HTTP).
- Si le paquet Accès-accepté contient un attribut Digest-HA1, le client RADIUS vérifie les directives qop et algorithme dans l'en-tête Autorisation de la demande de style HTTP qu'il veut autoriser :
  - Si la directive qop manque ou si sa valeur est "auth", le client RADIUS ignore l'attribut Digest-HA1. Il n'inclut pas d'en-tête Informations d'authentification dans sa réponse de style HTTP.
  - Si la valeur de la directive qop est "auth-int" et si au moins une des conditions suivantes est vraie, le client RADIUS calcule le contenu de la directive rspauth de la réponse de style HTTP :
    - La valeur de la directive algorithme est "MD5-sess" ou "AKAv1-MD5-sess".
    - La sécurité IP (IPsec) est configurée pour protéger le trafic entre le client RADIUS et le serveur RADIUS avec IPsec (voir la Section 8).

Le client RADIUS crée le message de réponse de style HTTP et calcule le hachage du corps de ce message. Il utilise le résultat et la valeur de l'attribut URI de résumé du paquet Demande d'accès correspondant pour effectuer le calcul de H(A2). Il prend les valeurs de Nom occasionnel de résumé, Compte de noms occasionnels de résumé, Digest-CNonce, et Qop de résumé de la Demande d'accès correspondante et la valeur de l'attribut Digest-HA1 pour finir le calcul de la valeur de rspauth.

- Si le paquet Accès-accepté ne contient ni un attribut Auth de réponse de résumé ni un attribut Digest-HA1, le client RADIUS ne va pas créer un en-tête Informations d'authentification pour sa réponse de style HTTP.

Quand le serveur RADIUS fournit un attribut Digest-Nextnonce dans le paquet Accès-accepté, le client RADIUS met le contenu de cet attribut dans une directive nextnonce. Il peut maintenant envoyer une réponse de style HTTP.

2.1.4 Échec d'authentification

Si le client RADIUS a bien reçu une demande de style HTTP sans un en-tête Autorisation(mandataire-) correspondant à sa valeur de domaine configurée en local, il obtient un nouveau nom occasionnel et envoie une réponse d'erreur (401 ou 407) contenant un en-tête Authentification(mandataire-).

Si le client RADIUS reçoit un paquet Défi d'accès en réponse à une Demande d'accès contenant un attribut Nom occasionnel de résumé, le serveur RADIUS n'a pas accepté le nom occasionnel. Si un attribut Résumé périmé est présent dans le Défi d'accès et a une valeur de "vrai" (sans les guillemets qui l'entourent) le client RADIUS envoie une réponse d'erreur (401 ou 407) contenant un en-tête WWW-/Proxy-Authenticate avec la directive Périmé réglée à "vrai" et les directives de résumé déduites des attributs Digest-*.

Si le client RADIUS reçoit un Accès-rejeté du serveur RADIUS, il envoie une réponse d'erreur à la demande de style HTTP qu'il a reçue. Si le client RADIUS ne reçoit pas de réponse, il retransmet ou se replie sur un autre serveur RADIUS comme décrit dans la [RFC2865].

2.1.5 Obtention des noms occasionnels

Le client RADIUS a deux façons d'obtenir des noms occasionnels : il en a reçu un dans l'attribut Digest-Nextnonce d'un paquet Accès-accepté reçu précédemment, ou il en demande un au serveur RADIUS. Pour faire cette demande, il envoie une Demande d'accès contenant un attribut Méthode de résumé et URI de résumé, mais sans attribut Nom occasionnel de résumé. Il ajoute un attribut Authentifiant de message (voir la [RFC3579]) au paquet Demande d'accès. Le serveur RADIUS choisit un nom occasionnel et répond avec un Défi d'accès contenant un attribut Nom occasionnel de résumé.

Le client RADIUS construit un en-tête Authentification(mandataire-) en utilisant les attributs Nom occasionnel de résumé et Domaine de résumé reçus pour remplir les directives Nom occasionnel et Domaine. Le serveur RADIUS peut envoyer des attributs Qop de résumé, Algorithme de résumé, Domaine de résumé, et Digest-Opaque dans le Défi d'accès qui porte le nom occasionnel. Si ces attributs sont présents, le client DOIT les utiliser.

2.2 Comportement du serveur RADIUS

Si le serveur RADIUS reçoit un paquet Demande d'accès avec un attribut Méthode de résumé et URI de résumé mais sans attribut Nom occasionnel de résumé, il choisit un nom occasionnel. Il met le nom occasionnel dans un attribut Nom occasionnel de résumé et l'envoie dans un paquet Défi d'accès au client RADIUS. Le serveur RADIUS DOIT ajouter les attributs Domaine de résumé, Authentifiant de message (voir la [RFC3579]) DEVRAIT ajouter Algorithme de résumé et un ou plusieurs Qop de résumé, et PEUT ajouter des attributs Domaine de résumé ou Digest-Opaque au paquet Défi d'accès.

2.2.1 Vérifications générales d'attributs

Si le serveur RADIUS reçoit un paquet Demande d'accès contenant un attribut Réponse de résumé, il cherche les attributs suivants : Domaine de résumé, Nom occasionnel de résumé, Méthode de résumé, URI de résumé, Qop de résumé, Algorithme de résumé, et Nom d'utilisateur de résumé. Selon le contenu de Algorithme de résumé et Qop de résumé, il cherche aussi Hachage de corps d'entité de résumé, Digest-CNonce, et Digest-AKA-Auts. Voir les détails dans les [RFC2617] et [RFC3310]. Si l'attribut Algorithme de résumé manque, "MD5" est supposé. Si le serveur RADIUS a produit un attribut Digest-Opaque avec le nom occasionnel, la Demande d'accès DOIT avoir un attribut Digest-Opaque correspondant.

Si des attributs obligatoires manquent, il DOIT répondre avec un paquet Accès-rejeté.

Le serveur RADIUS retire les caractères "\" qui échappent les guillemets et les caractères "\" des valeurs de texte qu'il a reçus dans les attributs Digest-*.

Si les attributs obligatoires sont présents, le serveur RADIUS DOIT vérifier si le client RADIUS est autorisé à desservir les utilisateurs du domaine mentionné dans l'attribut Domaine de résumé. Si le client RADIUS n'est pas autorisé, le serveur RADIUS DOIT envoyer un Accès-rejeté. Le serveur RADIUS DEVRAIT enregistrer les événements afin d'en notifier l'opérateur, et PEUT prendre des mesures supplémentaires comme d'envoyer un Accès-rejeté en réponse à toutes les futures demandes provenant de ce client, jusqu'à ce que ce comportement soit supprimé par une action de gestion.

Le serveur RADIUS détermine l'âge du nom occasionnel dans le Nom occasionnel de résumé en utilisant un horodatage incorporé ou en le cherchant dans un tableau local. Le serveur RADIUS DOIT vérifier l'intégrité du nom occasionnel si il incorpore l'horodatage dans le nom occasionnel. Le paragraphe 2.2.2 décrit comment le serveur traite les vieux noms occasionnels.

2.2.2 Authentification

Si le message Demande d'accès réussit la vérification décrite ci-dessus, le serveur RADIUS calcule la réponse de résumé comme décrit dans la [RFC2617]. Pour chercher le mot de passe, le serveur RADIUS utilise l'attribut RADIUS Nom d'utilisateur. Le serveur RADIUS DOIT vérifier si l'utilisateur identifié par l'attribut Nom d'utilisateur :

- o est autorisé à accéder à l'espace de protection et
- o est autorisé à utiliser l'URI inclus dans l'attribut SIP-AOR, si cet attribut est présent.

Si une ce ces vérifications échoue, le serveur RADIUS DOIT envoyer un Accès-rejeté.

La corrélation entre les valeurs d'AVP Nom d'utilisateur et SIP-AOR est exigée juste pour éviter qu'un utilisateur enregistre ou fasse un mauvais usage d'un SIP-AOR qui a été alloué à un utilisateur différent.

Toutes les valeurs requises pour le calcul de résumé sont prises dans les attributs Résumé décrits dans le présent document. Si la réponse de résumé calculée est égale à la valeur reçue dans l'attribut Réponse de résumé, l'authentification est réussie.

Si les valeurs de réponse correspondent, mais si le serveur RADIUS considère que le nom occasionnel dans l'attribut Nom occasionnel de résumé est trop vieux, il envoie un paquet Défi d'accès contenant un nouveau nom occasionnel et un attribut Résumé périmé avec une valeur de "vrai" (sans les guillements qui l'entourent).

Si les valeurs de réponse ne correspondent pas, le serveur RADIUS répond avec un Accès-rejeté.

2.2.3 Construction de la réponse

Si l'authentification a réussi, le serveur RADIUS ajoute un attribut au paquet Accès-accepté qui peut être utilisé par le client RADIUS pour construire un en-tête Informations d'authentification :

- o Si la valeur de l'attribut Qop de résumé est "auth" ou non spécifiée, le serveur RADIUS DEVRAIT mettre un attribut Auth de réponse de résumé dans le paquet Accès-accepté.
- o Si la valeur de l'attribut Qop de résumé est "auth-int" et si au moins une des conditions suivantes est vraie, le serveur RADIUS DEVRAIT mettre un attribut Digest-HA1 dans le paquet Accès-accepté :
  - * La valeur de l'attribut Algorithme de résumé est "MD5-sess" ou "AKAv1-MD5-sess".
  - * IPsec est configuré pour protéger le trafic entre le client et le serveur RADIUS avec IPsec (voir la Section 8).

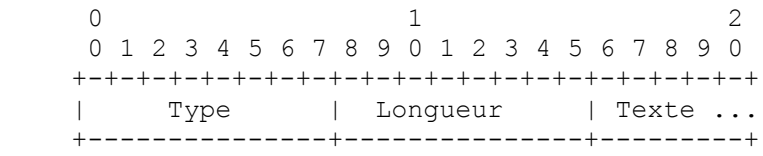
Dans tous les autres cas, Auth de réponse de résumé ou Digest-HA1 NE DOIT PAS être envoyé.

Les serveurs RADIUS PEUVENT construire un attribut Digest-Nextnonce *(prochain nom occasionnel de résumé)* et l'ajouter au paquet Accès-accepté. C'est utile pour limiter la durée de vie d'un nom occasionnel et pour économiser un aller-retour dans une future demande (voir la discussion de nextnonce dans la [RFC2617], paragraphe 3.2.3). Le serveur RADIUS ajoute un attribut Authentifiant de message (voir la [RFC3579]) et envoie le paquet Accès-accepté au client RADIUS.

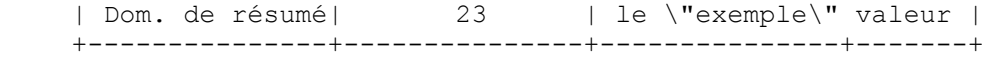
Si le serveur RADIUS n'accepte pas le nom occasionnel reçu dans un paquet Demande d'accès mais si l'authentification réussit, le serveur RADIUS DOIT envoyer un paquet Défi d'accès contenant un attribut Résumé périmé réglé à "vrai" (sans les guillemets qui l'entourent). Le serveur RADIUS DOIT ajouter les attributs Authentifiant de message (voir la [RFC3579]), Nom occasionnel de résumé, Domaine de résumé, DEVRAIT ajouter l'attribut Algorithme de résumé et un ou plusieurs Digest-Qop, et PEUT ajouter les attributs Domaine de résumé ou Digest-Opaque au paquet Défi d'accès.

3. Nouveaux attributs RADIUS

Sauf mention contraire, les attributs ont le format suivant :



Les caractères guillemets et barre oblique dans les attributs Digest-* représentant des directives de style HTTP avec une syntaxe de chaîne entre guillemets sont échappées. Les guillemets sont supprimés. Ce sont des délimiteurs syntaxiques qui sont redondants dans RADIUS. Par exemple, la directive realm="le \"exemple\" valeur" est représentée comme suit :



3.1 Attribut Réponse de résumé

Description : Si cet attribut est présent dans un message Demande d'accès, un serveur RADIUS qui met en œuvre la présente spécification DOIT traiter la demande d'accès comme une demande d'authentification par résumé. Quand un client RADIUS reçoit un en-tête (Mandataire-)Autorisation, il met la valeur de Demande-résumé dans un attribut Réponse de résumé. Cet attribut (qui permet à l'utilisateur de prouver la possession du mot de passe) DOIT seulement être utilisé dans les paquets Demande d'accès.

Type : 103 pour Réponse de résumé.

Longueur : ≥ 3

Texte : Quand on utilise le résumé HTTP, le champ Texte est long de 32 octets et contient une représentation hexadécimale d'une valeur de 16 octets telle que calculée par le client authentifié. D'autres algorithmes de résumé PEUVENT définir des longueurs de résumé différentes. Le champ Texte DOIT être copié du résumé de demande de la réponse de résumé [RFC2617] sans guillemets autour.

3.2 Attribut Domaine de résumé

Description : cet attribut décrit un composant d'espace de protection du serveur RADIUS. Les protocoles de style HTTP diffèrent dans leur définition de l'espace de protection. Voir les détails au paragraphe 1.2 de la [RFC2617]. Il DOIT seulement être utilisé dans les paquets Demande d'accès, Défi d'accès, et Demande de comptabilité.

Type : 104 pour Domaine de résumé

Longueur : ≥ 3

Texte : dans les demandes d'accès, le client RADIUS prend la valeur de la directive domaine (valeur de domaine conformément à la [RFC2617]) sans guillemets autour, provenant de la demande de style HTTP qu'il veut authentifier. Dans les paquets Défi d'accès, le serveur RADIUS met la valeur de domaine attendue dans cet attribut.

3.3 Attribut Nom occasionnel de résumé

Description : cet attribut contient un nom occasionnel à utiliser dans le calcul du résumé HTTP. Si la demande d'accès a une méthode de résumé et un URI de résumé mais pas d'attribut Nom occasionnel de résumé, le serveur RADIUS DOIT mettre un attribut Nom occasionnel de résumé dans son paquet Défi d'accès. Cet attribut DOIT seulement être utilisé dans les paquets Demande d'accès et Défi d'accès.

Type : 105 pour Nom occasionnel de résumé

Longueur : ≥ 3

Texte : dans les demandes d'accès, le client RADIUS prend la valeur de la directive de nom occasionnel (valeur de nom occasionnel dans la [RFC2617]) sans guillemets autour, provenant de la demande de style HTTP qu'il veut authentifier. Dans les paquets Défi d'accès, l'attribut contient le nom occasionnel choisi par le serveur RADIUS.

3.4 Attribut Auth de réponse de résumé

Description : cet attribut permet au serveur RADIUS de prouver la possession du mot de passe. Si l'attribut précédemment reçu Qop de résumé était "auth-int" (sans guillemets autour) le serveur RADIUS DOIT envoyer un attribut Digest-HA1 à la place d'un attribut Auth de réponse de résumé. L'attribut Auth de réponse de résumé DOIT seulement être utilisé dans les paquets Accès-accepté. Le client RADIUS met la valeur d'attribut sans guillemets autour dans la directive rspauth de l'en-tête Informations d'authentification.

Type : 106 pour Auth de réponse de résumé.

Longueur : ≥ 3

Texte : le serveur RADIUS calcule un résumé conformément au paragraphe 3.2.3 de la [RFC2617] et copie le résultat dans cet attribut. Des algorithmes de résumé autres que celui défini dans la [RFC2617] PEUVENT définir des longueurs de résumé autres que 32.

3.5 Attribut Digest-Nextnonce

Cet attribut contient un nom occasionnel à utiliser dans le calcul du résumé HTTP.

Description : le serveur RADIUS PEUT mettre un attribut Digest-Nextnonce dans un paquet Accès-accepté. Si cet attribut est présent, le client RADIUS DOIT mettre le contenu de cet attribut dans la directive nextnonce d'un en-tête Informations d'authentification dans sa réponse de style HTTP. Cet attribut DOIT seulement être utilisé dans les paquets Accès-accepté.

Type : 107 pour Digest-Nextnonce

Longueur : ≥ 3

Texte : il est recommandé que ce texte soit en données en base64 ou hexadécimal.

3.6 Attribut Méthode de résumé

Description : cet attribut contient la valeur de la méthode à utiliser dans le calcul du résumé HTTP. Cet attribut DOIT seulement être utilisé dans les paquets Demande d'accès et Demande de comptabilité.

Type : 108 pour Méthode de résumé

Longueur : ≥ 3

Texte : dans les demandes d'accès, le client RADIUS prend la valeur de la méthode de demande de la demande de style HTTP qu'il veut authentifier.

3.7 Attribut URI de résumé

Description : cet attribut est utilisé pour transporter le contenu de la directive digest-uri ou de l'URI de la demande de style HTTP. Il DOIT seulement être utilisé dans les paquets Demande d'accès et Demande de comptabilité.

Type : 109 pour URI de résumé

Longueur : ≥ 3

Texte : si la demande de style HTTP a un en-tête Autorisation, le client RADIUS met la valeur de la directive uri trouvée dans l'en-tête Autorisation de la demande de style HTTP (connue comme "digest-uri-value" au paragraphe 3.2.2 de la [RFC2617]) sans guillemets autour dans cet attribut. Si il n'y a pas d'en tête Autorisation, le client RADIUS prend la valeur de l'URI de demande de la demande de style HTTP qu'il veut authentifier.

3.8 Attribut Qop de résumé

Description : cet attribut contient le paramètre Qualité de protection qui influence le calcul du résumé HTTP. Cet attribut DOIT seulement être utilisé dans les paquets Demande d'accès, Défi d'accès, et Demande de comptabilité. Un client RADIUS DEVRAIT insérer un des attributs Qop de résumé qu'il a reçu dans un précédent paquet Défi d'accès. Les serveurs RADIUS DEVRAIENT insérer au moins un attribut Qop de résumé dans un paquet Défi d'accès. Qop de résumé est facultatif afin de préserver la rétro compatibilité avec une mise en œuvre minimale de la [RFC2069].

Type : 110 pour Qop de résumé

Longueur : ≥ 3

Texte : dans les demandes d'accès, le client RADIUS prend la valeur de la directive qop (qop-value comme décrit dans la [RFC2617]) de la demande de style HTTP qu'il veut authentifier. Dans les paquets Défi d'accès, le serveur RADIUS met une valeur de qop désirée dans cet attribut. Si le serveur RADIUS supporte plus d'une valeur de "qualité de protection", il met chaque valeur de qop dans un attribut Qop de résumé séparé.

3.9 Attribut Algorithme de résumé

Description : cet attribut contient le paramètre Algorithme qui influence le calcul du résumé HTTP. Il DOIT seulement être utilisé dans les paquets Demande d'accès, Défi d'accès et Demande de comptabilité. Si cet attribut manque, MD5 est supposé.

Type : 111 pour Algorithme de résumé

Longueur : ≥ 3

Texte : dans les demandes d'accès, le client RADIUS prend la valeur de la directive algorithme (comme décrit au paragraphe 3.2.1 de la [RFC2617]) de la demande de style HTTP qu'il veut authentifier. Dans les paquets Défi d'accès, le serveur RADIUS DEVRAIT mettre l'algorithme désiré dans cet attribut.

3.10 Attribut Hachage de corps d'entité de résumé

Description : quand on utilise la valeur de qop de "auth-int", un hachage du contenu du corps de message de style HTTP est exigé pour le calcul du résumé. Au lieu d'envoyer le corps complet du message, on envoie seulement sa valeur de hachage. Cette valeur de hachage peut être utilisée directement dans le calcul de résumé. Les éclaircfssements décrits au paragraphe 22.4 de la [RFC3261] sur le hachage de corps d'entités vides s'appliquent à l'attribut Hachage de corps d'entité de résumé. Cet attribut DOIT seulement être envoyé dans les paquets Demande d'accès.

Type : 112 pour Hachage de corps d'entité de résumé

Longueur : ≥ 3

Texte : l'attribut contient la représentation hexadécimale de H(corps d'entité). Ce hachage est exigé par certains mécanismes d'authentification, comme le résumé HTTP avec la qualité de protection réglée à "auth-int". Les clients RADIUS DOIVENT utiliser cet attribut pour transporter le hachage du corps d'entité quand le résumé HTTP est le mécanisme d'authentification et que le serveur RADIUS exige que l'intégrité du corps de l'entité (par exemple, le paramètre qop réglé à "auth-int") soit vérifiée. Des extensions au présent document pourront définir la prise en charge de mécanismes d'authentification autres que le résumé HTTP.

3.11 Attribut Digest-CNonce

Description : cet attribut contient le paramètre Nom occasionnel de client qui est utilisé dans le calcul du résumé HTTP. Il DOIT seulement être utilisé dans les paquets Demande d'accès.

Type : 113 pour Digest-CNonce

Longueur : ≥ 3

Texte : cet attribut inclut la valeur de cnonce-value [RFC2617] sans guillemets autour, tirée de la demande de style HTTP.

3.12 Attribut Compte de noms occasionnels de résumé

Description : cet attribut inclut le paramètre Compte de noms occasionnels qui est utilisé pour détecter les attaques en répétition. L'attribut DOIT seulement être utilisé dans les paquets Demande d'accès.

Type : 114 pour Compte de noms occasionnels de résumé

Longueur : 10

Texte : dans les demandes d'accès, le client RADIUS prend la valeur de la directive nc (nc-value selon la [RFC2617]) sans guillemets autour, de la demande de style HTTP qu'il veut authentifier.

3.13 Attribut Nom d'utilisateur de résumé

Description : cet attribut contient le nom d'utilisateur utilisé dans le calcul de résumé HTTP. Le serveur RADIUS DOIT utiliser cet attribut seulement pour les besoins du calcul du résumé. Afin de déterminer les accréditifs d'utilisateur appropriés, le serveur RADIUS DOIT utiliser l'attribut Nom d'utilisateur (1) et NE DOIT PAS utiliser l'attribut Nom d'utilisateur de résumé. Cet attribut DOIT seulement être utilisé dans les paquets Demande d'accès et Demande de comptabilité.

Type : 115 pour Nom d'utilisateur de résumé

Longueur : ≥ 3

Texte : dans les demandes d'accès, le client RADIUS prend la valeur de la directive username (username-value selon la [RFC2617]) sans guillemets autour de la demande de style HTTP qu'il veut authentifier.

3.14 Attribut Digest-Opaque

Description : cet attribut contient le paramètre opaque qui est passé au client de style HTTP. Le client de style HTTP va repasser cette valeur au serveur (c'est-à-dire, le client RADIUS) sans modification. Cet attribut DOIT seulement être utilisé dans les paquets Demande d'accès et Défi d'accès.

Type : 116 pour Digest-Opaque

Longueur : ≥ 3

Texte : dans les demandes d'accès, le client RADIUS prend la valeur de la directive opaque (opaque-value selon la [RFC2617]) sans guillemets autour de la demande de style HTTP qu'il veut authentifier et la met dans cet attribut. Dans les paquets Défi d'accès, le serveur RADIUS PEUT inclure cet attribut.

3.15 Attribut Digest-Auth-Param

Description : cet attribut est un fourre-tout pour de futures extensions et correspond au paramètre auth-param défini au paragraphe 3.2.1 de la [RFC2617]. Digest-Auth-Param est le mécanisme par lequel le client et le serveur RADIUS peuvent échanger des paramètres d'extension auth-param contenus dans les en-têtes Digest qui ne sont pas compris par le client RADIUS et pour lesquels il n'y a pas d'attribut autonome correspondant. À la différence des attributs Digest-* précédemment mentionnés, Digest-Auth-Param contient non seulement la valeur mais aussi le nom du paramètre, car celui-ci n'est pas connu du client RADIUS. Si l'en-tête Digest contient plusieurs paramètres inconnus, alors la mise en œuvre RADIUS DOIT répéter cet attribut, et chaque instance DOIT contenir une combinaison différente de paramètre/valeur de résumé inconnue. Cet attribut DOIT SEULEMENT être utilisé dans les paquets Demande d'accès, Défi d'accès, Accès-accepté, et Demande de comptabilité.

Type : 117 pour Digest-Auth-Param

Longueur : ≥ 3

Texte : le texte consiste en le paramètre entier, incluant son nom, le signe égal ("="), et les guillemets.

3.16 Attribut Digest-AKA-Auts

Description : cet attribut contient le paramètre auts qui est utilisé dans le calcul du résumé AKA [RFC3310]. Il est seulement utilisé si l'algorithme de réponse de résumé note une version de résumé AKA [RFC3310]. Cet attribut DOIT seulement être utilisé dans les paquets Demande d'accès.

Type : 118 pour Digest-AKA-Auts

Longueur : ≥ 3

Texte : dans les demandes d'accès, le client RADIUS prend la valeur de la directive auts (auts-param selon le paragraphe 3.4 de la [RFC3310]) sans guillemets autour, de la demande de style HTTP qu'il veut authentifier.

3.17 Attribut Domaine de résumé

Description : Quand un client RADIUS a demandé un nom occasionnel, le serveur RADIUS PEUT envoyer un ou plusieurs attributs Domaine de résumé dans son paquet Défi d'accès. Le client RADIUS les met dans la liste entre guillemets, séparée par des espaces, des URI de la directive domaine d'un en-tête WWW-Authenticate. Avec le domaine de résumé, les URI dans la liste définissent l'espace de protection (voir le paragraphe 3.2.1 de la [RFC2617]) pour des protocoles de style HTTP. Cet attribut DOIT seulement être utilisé dans les paquets Défi d'accès et Demande de comptabilité.

Type : 119 pour Domaine de résumé.

Longueur : 3

Texte : cet attribut consiste en un seul URI qui définit un composant d'espace de protection.

3.18 Attribut Résumé périmé

Description : cet attribut est envoyé par un serveur RADIUS afin de notifier au client RADIUS qu'il a accepté un nom occasionnel. Si le nom occasionnel présenté par le client RADIUS était périmé, la valeur est "vrai" et est "faux" autrement. Le client RADIUS met le contenu de cet attribut dans une directive "stale" de l'en-tête WWW-Authenticate dans la réponse de style HTTP à la demande qu'il veut authentifier. L'attribut DOIT seulement être utilisé dans les paquets Défi d'accès.

Type : 120 pour Résumé périmé.

Longueur : 3

Texte : l'attribut a la valeur "vrai" ou "faux" (les deux valeurs sans guillemets autour).

3.19 Attribut Digest-HA1

Description : cet attribut est utilisé pour permettre la génération d'un en-tête Informations d'authentification, même si le corps de la réponse de style HTTP est exigé pour le calcul de la valeur rspauth. Il DEVRAIT être utilisé dans les paquets Accès-accepté si la qualité de protection (qop) requise est "auth-int". Cet attribut NE DOIT PAS être envoyé si le paramètre qop n'était pas spécifié ou a une valeur de "auth" (dans ce cas, on utilise à la place Authentification de réponse de résumé). L'attribut Digest-HA1 DOIT seulement être envoyé par le serveur RADIUS ou traité par le client RADIUS si au moins une des conditions suivantes est vraie :

+ La valeur de l'attribut Algorithme de résumé est "MD5-sess" ou "AKAv1-MD5-sess".
+ IPsec est configuré à protéger le trafic entre le client et le serveur RADIUS avec IPsec (voir la Section 8).

Cet attribut DOIT seulement être utilisé dans les paquets Accès-accepté.

Type : 121 pour Digest-HA1.

Longueur : ≥ 3

Texte : cet attribut contient la représentation hexadécimale de H(A1) comme décrit aux paragraphes 3.1.3, 3.2.1, et 3.2.2.2 de la [RFC2617].

3.20 Attribut SIP-AOR

Description : cet attribut est utilisé pour l'autorisation des messages SIP. L'attribut SIP-AOR identifie l'URI, dont l'utilisation doit être authentifiée et autorisée. Le serveur RADIUS utilise cet attribut pour autoriser le traitement de la demande SIP. Le SIP-AOR peut être déduit, par exemple, du champ d'en-tête To dans une demande SIP REGISTER (utilisateur qui s'enregistre) ou du champ d'en-tête From dans une autre demande SIP. Cependant, la transposition exacte de cet attribut en SIP peut changer du fait de nouveaux développements dans le protocole. Cet attribut DOIT seulement être utilisé quand le client RADIUS veut autoriser les utilisateurs SIP et DOIT seulement être utilisé dans les paquets Demande d'accès.

Type : 122 pour SIP-AOR.

Longueur : ≥ 3

Texte : la syntaxe de cet attribut correspond soit à un URI SIP (avec le format défini dans la [RFC3261], soit à un URI tel (avec le format défini dans la [RFC3966]). L'attribut SIP-AOR contient l'URI complet, incluant les paramètres et autres parties. ll appartient au serveur RADIUS de décider quels composants de l'URI sont considérés dans la décision d'autorisation.

4. Compatibilité avec Diameter

Le présent document définit la prise en charge de l'authentification par résumé dans RADIUS. Un document d'accompagnement, "Application Diameter du protocole d'initialisation de session (SIP)" [RFC4740] définit la prise en charge de l'authentification par résumé dans Diameter, et traite les questions de compatibilité entre RADIUS et Diameter.

5. Tableau des attributs

Le tableau suivant est un guide des attributs qui peuvent être trouvés dans quels types de paquets, et en quelle quantité.

n°	Attribut	Demande d'accès	Accès accepté	Accès rejeté	Défi d'accès	Req
1	Nom d'utilisateur	0	0	0	0	0-1
24	État [4]	0-1	0	0	1	0
80	Authentifiant de message	1	1	1	1	0-1
103	Réponse de résumé	0-1	0	0	0	0
104	Domaine de résumé	0-1	0	0	1	0-1
105	Nom occasionnel de résumé	0-1	0	0	1	0
106	Auth de réponse de résumé [1], [2]	0	0-1	0	0	0
107	Prochain nom occasionnel de résumé	0	0-1	0	0	0
108	Méthode de résumé	1	0	0	0	0-1
109	URI de résumé	0-1	0	0	0	0-1
110	Qop de résumé	0-1	0	0	0	0-1
111	Algorithme de résumé [3]	0-1	0	0	0-1	0-1
112	Hachage de corps d'entité de résumé	0-1	0	0	0	0
113	Digest-CNonce	0-1	0	0	0	0
114	Compte de noms occasionnels de résumé	0-1	0	0	0	0
115	Nom d'utilisateur de résumé	0-1	0	0	0	0-1
116	Digest-Opaque	0-1	0	0	0-1	0
117	Digest-Auth-Param	0	0	0	0	0
118	Digest-AKA-Auts	0-1	0	0	0	0
119	Domaine de résumé	0	0	0	0	0
120	Résumé périmé	0	0	0	0-1	0
121	Digest-HA1 [1], [2]	0	0-1	0	0	0
122	SIP-AOR	0-1	0	0	0	0

Signification des entrés du tableau :
0 : cet attribut NE DOIT PAS être présent dans le paquet.
0+ : zéro, une ou plusieurs instances de cet attribut PEUVENT être présentes dans le paquet.
0-1 : zéro, une ou plusieurs instances de cet attribut PEUVENT être présentes dans le paquet.

[Note 1] Digest-HA1 DOIT être utilisé à la place de Auth de réponse de résumé si Qop de résumé est "auth-int".
[Note 2] Auth de réponse de résumé DOIT être utilisé à la place de Digest-HA1 si Qop de résumé est "auth".
[Note 3] Si Algorithme de résumé manque, "MD5" est supposé.
[Note 4] Un Défi d'accès DOIT contenir un attribut État, qui est copié dans la demande d'accès suivante. Un serveur qui reçoit une demande d'accès qui contient un attribut État DOIT répondre avec un Accès-accepté ou un Accès-rejeté ; le serveur NE DOIT PAS répondre avec un Défi d'accès.

6. Exemples

Voici un exemple de trafic entre un téléphone intelligent (A), un serveur mandataire (B), et un serveur RADIUS exemple.com (C). La communication entre le serveur mandataire et une passerelle entre SIP et le réseau téléphonique public commuté 'RTPC) est omise pour rester concis. Les messages SIP ne sont pas montrés complètement.

Le mot de passe de l'utilisateur '12345678' est 'secret'. Le secret partagé entre le client et le serveur RADIUS est 'secret'. Pour faciliter l'essai, seulement le dernier octet de l'authentifiant RADIUS change entre les demandes. Dans une mise en œuvre réelle, ce serait une faute grave.

A->B
INVITE sip:97226491335@exemple.com SIP/2.0
From: <sip:12345678@exemple.com>
To: <sip:97226491335@exemple.com>

B->A
SIP/2.0 100 Essai

B->C
Code = Demande d'accès (1)
Identifiant de paquet = 0x7c (124)
Longueur = 97
Authentifiant = F5E55840E324AA49D216D9DBD069807C
Adresse IP de NAS = 192.0.2.38
Accès de NAS = 5
Nom d'utilisateur = 12345678
Méthode de résumé = INVITE
URI de résumé = sip:97226491335@exemple.com
Authentifiant de message = 7600D5B0BDC33987A60D5C6167B28B3B

C->B
Code = Défi d'accès (11)
Identifiant de paquet = 0x7c (124)
Longueur = 72
Authentifiant = EBE20199C26EFEAD69BF8AB0E786CA4D
Nom occasionnel de résumé = 3bada1a0
Domaine de résumé = exemple.com
Qop de résumé = auth
Algorithme de résumé = MD5
Authentifiant de message = 5DA18ED3BBC9513DCBDE0A37F51B7DE3

B->A
SIP/2.0 407 Authentification de mandataire exigée
Authentification de mandataire : Domaine de résumé="exemple.com"
,nom occasionnel="3bada1a0",qop=auth,algorithme=MD5
Longueur de contenu : 0

A->B
ACK sip:97226491335@exemple.com SIP/2.0

A->B
INVITE sip:97226491335@exemple.com SIP/2.0
Autorisation de mandataire : nom occasionnel de résumé="3bada1a0"
,domaine="exemple.com"
,réponse="756933f735fcd93f90a4bbdd5467f263"
,uri="sip:97226491335@exemple.com",username="12345678"
,qop=auth,algorithme=MD5
,cnonce="56593a80,nc="00000001"
From: <sip:12345678@exemple.com>
To: <sip:97226491335@exemple.com>

B->C
Code = Demande d'accès (1)
Identifiant de paquet = 0x7d (125)
Longueur = 221
Authentifiant = F5E55840E324AA49D216D9DBD069807D
Adresse IP de NAS = 192.0.2.38
Accès de NAS = 5
Nom d'utilisateur = 12345678
Méthode de résumé = INVITE
URI de résumé = sip:97226491335@exemple.com
Domaine de résumé = exemple.com
Qop de résumé = auth
Algorithme de résumé = MD5
Digest-CNonce = 56593a80

Nom occasionnel de résumé = 3bada1a0
Compte de noms occasionnels de résumé = 00000001
Réponse de résumé = 756933f735fcd93f90a4bbdd5467f263
Nom d'utilisateur de résumé = 12345678
SIP-AOR = sip:12345678@exemple.com
Authentifiant de message = B6C7F7F8D11EF261A26933D234561A60

C->B
Code = Accès-accepté (2)
Identifiant de paquet = 0x7d (125)
Longueur = 72
Authentifiant = FFDD74D6470D21CB6FC4D6056BE245D2
Auth de réponse de résumé = f847de948d12285f8f4199e366f1af21
Authentifiant de message = 7B76E2F10A7067AF601938BF13B0A62E

B->A
SIP/2.0 180 Sonnerie

B->A
SIP/2.0 200 OK

A->B
ACK sip:97226491335@exemple.com SIP/2.0

Un second exemple montre le trafic entre un navigateur de la Toile (A), un serveur de la Toile (B), et un serveur RADIUS (C).

A->B
GET /index.html HTTP/1.1

B->C
Code = Demande d'accès (1)
Identifiant de paquet = 0x7e (126)
Longueur = 68
Authentifiant = F5E55840E324AA49D216D9DBD069807E
Adresse IP de NAS = 192.0.2.38
Accès de NAS = 5
Méthode de résumé = GET
URI de résumé = /index.html
Authentifiant de message = 690BFC95E88DF3B185F15CD78E469992

C->B
Code = Défi d'accès (11)
Identifiant de paquet = 0x7e (126)
Longueur = 72
Authentifiant = 2EE5EB01C02C773B6C6EC8515F565E8E
Nom occasionnel de résumé = a3086ac8
Domaine de résumé = exemple.com
Qop de résumé = auth
Algorithme de résumé = MD5
Authentifiant de message = 646DB2B0AF9E72FFF2CF7FEB33C4952A

B->A
HTTP/1.1 401 Authentification exigée
WWW-Authenticate : Domaine de résumé="exemple.com",
nom occasionnel="a3086ac8",qop=auth,algorithme=MD5
Longueur de contenu : 0

A->B
GET /index.html HTTP/1.1

Autorisation : Digest = algorithme=MD5,qop=auth,nom occasionnel="a3086ac8"
,nc="00000001",cnonce="56593a80"
,domaine="exemple.com"
,réponse="a4fac45c27a30f4f244c54a2e99fa117"
,uri="/index.html",nom d'utilisateur="12345678"

B->C
Code = Demande d'accès (1)
Identifiant de paquet = 0x7f (127)
Longueur = 176
Authentifiant = F5E55840E324AA49D216D9DBD069807F
Adresse IP de NAS = 192.0.2.38
Accès de NAS = 5
Nom d'utilisateur = 12345678
Méthode de résumé = GET
URI de résumé = /index.html
Domaine de résumé = exemple.com
Qop de résumé = auth
Algorithme de résumé = MD5
Digest-CNonce = 56593a80
Nom occasionnel de résumé = a3086ac8
Compte de noms occasionnels de résumé = 00000001
Réponse de résumé = a4fac45c27a30f4f244c54a2e99fa117
Nom d'utilisateur de résumé = 12345678
Authentifiant de message = 237D85C1478C70C67EEAF22A9C456821

C->B
Code = Accès-accepté (2)
Identifiant de paquet = 0x7f (127)
Longueur = 72
Authentifiant = 6364FA6ED66012847C05A0895607C694
Auth de réponse de résumé = 08c4e942d1d0a191de8b3aa98cd35147
Authentifiant de message = 43795A3166492AD2A890AD57D5F97D56

B->A
HTTP/1.1 200 OK
...
<html>
...

7. Considérations relatives à l'IANA

Les valeurs suivantes provenant de l'espace de nombres de types d'attribut RADIUS ont été allouées dans la [RFC4590]. Le présent document demande que les valeurs du tableau ci-dessous soient entrées dans le registre existant.

Attribut	**n°**
Réponse de résumé	103
Domaine de résumé	104
Nom occasionnel de résumé	105
Auth de réponse de résumé	106
Prochain nom occasionnele de résumé	107
Méthode de résumé	108
URI de résumé	109
Qop de résumé	110
Algorithme de résumé	111
Hachage de corps d'entité de résumé	112
Digest-CNonce	113
Compte de noms occasionnels de résumé	114
Nom d'utilisateur de résumé	115

Digest-Opaque	116
Digest-Auth-Param	117
Digest-AKA-Auts	118
Domaine de résumé	119
Résumé périmé	120
Digest-HA1	121
SIP-AOR	122

8. Considérations sur la sécurité

Les extensions à RADIUS décrites dans le présent document permettent à RADIUS de transporter les données requises pour effectuer un calcul de résumé. Par suite, RADIUS hérite des vulnérabilités du résumé HTTP (voir la [RFC2617], Section 4) en plus des vulnérabilités de la sécurité de RADIUS décrites dans la [RFC2865], Section 8, et dans la [RFC3579], Section 4.

Un attaquant qui compromet un client ou mandataire RADIUS peut mener des attaques par interposition même si les chemins entre A, B et B, C (Figure 2) ont été sécurisés avec TLS ou IPsec.

Le serveur RADIUS DOIT vérifier l'attribut Domaine de résumé qu'il a reçu d'un client. Si le client RADIUS n'est pas autorisé à desservir les clients de style HTTP de ce domaine, il pourrait être compromis.

8.1 Déni de service

Les clients RADIUS qui mettent en œuvre les extensions décrites dans le présent document peuvent authentifier la demande de style HTTP reçue sur l'Internet. Comparée à l'utilisation de RADIUS pour authentifier l'accès réseau de couche de liaison, les attaquants peuvent trouver plus facile de cacher leurs traces dans un tel scénario.

Un attaquant peut tenter une attaque de déni de service sur un ou plusieurs serveurs RADIUS en envoyant un grand nombre de demandes de style HTTP. Pour rendre plus difficiles les attaques de déni de service simples, le serveur RADIUS DOIT vérifier si il a généré le nom occasionnel reçu d'un client de style HTTP. Ceci DEVRAIT être fait sans état. Par exemple, un nom occasionnel pourrait consister en une partie cryptographiquement aléatoire et une sorte de signature fournie par le client RADIUS, comme décrit dans la [RFC2617], paragraphe 3.2.1.

8.2 Confidentialité et intégrité des données

Les attributs décrits dans le présent document sont envoyés en clair. Les serveurs RADIUS DEVRAIENT inclure les attributs Qop de résumé et Algorithme de résumé dans les messages Défi d'accès. Un interposé peut modifier ou supprimer ces attributs dans une attaque en dégradation, causant l'utilisation par le client RADIUS d'un schéma d'authentification plus faible que prévu.

L'attribut Authentifiant de message, décrit dans la [RFC3579], paragraphe 3.2, DOIT être inclus dans les messages Demande d'accès, Défi d'accès, Accès-rejeté, et Accès-accepté qui contiennent les attributs décrits dans cette spécification.

L'attribut Digest-HA1 ne contient pas de composant aléatoire si l'algorithme est 'MD5' ou 'AKAv1-MD5'. Cela rend plus faciles les attaques de dictionnaire hors ligne et permet des attaques en répétition.

Certaines combinaisons de paramètres exigent la protection des paquets RADIUS contre l'espionnage et l'altération. Les mises en œuvre DEVRAIENT essayer de déterminer automatiquement si IPsec est configuré pour protéger le trafic entre le client RADIUS et le serveur RADIUS. Si ce n'est pas possible, la mise en œuvre vérifie qu'un paramètre de configuration dit si IPsec va protéger le trafic RADIUS. La valeur par défaut de ce paramètre de configuration dit à la mise en œuvre que les paquets RADIUS ne seront pas protégés.

Les clients de style HTTP peuvent utiliser TLS avec les certificats côté serveur avec l'authentification par résumé HTTP. Au lieu de TLS, IPsec peut aussi être utilisé. TLS ou IPsec sécurisent la connexion tandis que l'authentification par résumé authentifie l'utilisateur. La transaction RADIUS peut être regardée comme une branche du chemin entre le client de style HTTP et le serveur de style HTTP. Pour empêcher RADIUS de représenter le maillon faible, le client RADIUS qui reçoit une demande de style HTTP via TLS ou IPsec pourrait utiliser une connexion également sécurisée avec le serveur RADIUS. Il y a plusieurs façons de réaliser cela, par exemple :

- le client RADIUS peut rejeter la demande de style HTTP reçue sur TLS ou IPsec,
- le client RADIUS peut exiger que le trafic soit envoyé et reçu sur IPsec.

RADIUS sur IPsec, si il est utilisé, DOIT se conformer aux exigences décrites dans la [RFC3579], paragraphe 4.2.

9. Références

9.1 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)

[RFC2617] J. Franks et autres, "Authentification HTTP : Authentification d'accès de base et par résumé", juin 1999. *(DS.)*

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. (*MàJ par* RFC2868, RFC3575, RFC5080, RFC8044) *(D.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)

[RFC3579] B. Aboba, P. Calhoun, "Prise en charge du protocole d'authentification extensible (EAP) par RADIUS", septembre 2003. (*MàJ par* RFC5080) *(Information)*

[RFC3966] H. Schulzrinne, "L'URI tel pour les numéros de téléphone", décembre 2004. (*MàJ par* RFC5341) *(P.S.)*

9.2 Références pour information

[RFC1994] W. Simpson, "Protocole d'authentification par mise en cause de la prise de contact en PPP (CHAP)", août 1996.

[RFC2069] J. Franks et autres, "Extension à HTTP : authentification d'accès par résumé", janvier 1997. (*Obs., voir* RFC2617) *(P.S.)*

[RFC3310] A. Niemi, J. Arkko, V. Torvinen, "Authentification de résumé dans le protocole de transfert Hypertext (HTTP) utilisant l'authentification et l'accord de clés (AKA)", septembre 2002. *(Information)*

[RFC3588] P. Calhoun et autres, "Protocole fondé sur Diameter", septembre 2003. (*Remplacée par la* RFC6733) *(P.S.)*

[RFC3851] B. Ramsdell, "Spécification du message d'extensions de messagerie Internet multi-objets/sécurisé (S/MIME) version 3.1", juillet 2004. *(Obsolète, voir* RFC5751)

[RFC4346] T. Dierks et E. Rescorla, "Protocole de sécurité de la couche Transport (TLS) version 1.1", avril 2006. *(Remplace* RFC2246 *; Remplacée par* RFC5246 *; MàJ par* RFC4366, 4680, 4681, 5746, 6176, 7465, 7507, 7919)

[RFC4590] B. Sterman et autres, "Extension à RADIUS pour l'authentification par résumé", juillet 2006.(*Obsolète, voir* RFC5090) *(P.S.)*

[RFC4740] M. Garcia-Martin et autres, "Application Diameter dans le protocole d'initialisation de session (SIP)", novembre 2006. *(P.S.)*

Appendice A. Changements par rapport à la RFC 4590

Cet Appendice fait la liste des changements majeurs entre la [RFC4590] et le présent document. Les changements mineurs, incluant style, grammaire, orthographe, et rédactionnels ne sont pas mentionnés ici.

- Le Tableau des attributs (Section 5) indique maintenant que l'attribut Méthode de résumé est exigé dans une Demande d'accès. Aussi, une entrée a été ajoutée pour l'attribut État. Le tableau inclut aussi des entrées pour les messages Demande de comptabilité. Comme noté dans les exemples, l'attribut Nom d'utilisateur n'est pas nécessaire quand on demande un nom occasionnel.

- Deux erreurs d'allocation d'attribut ont été corrigées dans les Considérations relatives à l'IANA (Section 7). L'attribut Authentification de réponse de résumé est le 106, et Prochain nom occasionnel de résumé est le numéro 107.

- Plusieurs erreurs ont été corrigés dans les exemples.

Remerciements

Les auteurs remercient Mike McCauley de son aide sur les détails des exemples.
Merci à Kevin McDermott (Cisco Systems) de ses commentaires et de sa mise en œuvre expérimentale.
Merci à tous les relecteurs, en particulier Miguel Garcia, Jari Arkko, Avi Lior, et Jun Wang.

Adresse des auteurs

Baruch Sterman
Kayote Networks
P.O. Box 1373
Efrat 90435
Israel
mél : baruch@kayote.com

Daniel Sadolevsky
SecureOL, Inc.
Jerusalem Technology Park
P.O. Box 16120
Jerusalem 91160
Israel
mél : dscreat@dscreat.com

David Williams
Cisco Systems
7025 Kit Creek Road
P.O. Box 14987
Research Triangle Park NC 27709
USA
mél : dwilli@cisco.com

David Schwartz
Kayote Networks
P.O. Box 1373
Efrat 90435
Israel
mél : david@kayote.com

Wolfgang Beck
Deutsche Telekom AG
Deutsche Telekom Allee 7
Darmstadt 64295
Germany
mél : beckw@t-systems.com

Déclaration complète de droits de reproduction

mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

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