Groupe de travail Réseau
Request for Comments : 3579
RFC mise à jour : 2869
Catégorie : Information

B. Aboba, Microsoft
P. Calhoun, Airespace
septembre 2003
Traduction Claude Brière de L'Isle

Prise en charge du protocole d'authentification extensible (EAP) par RADIUS

Statut de ce mémoire
Le présent mémoire apporte des informations pour la communauté de l'Internet. Le présent mémoire ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document définit la prise en charge par le service d'authentification à distance de l'utilisateur appelant (RADIUS, *Remote Authentication Dial In User Service*) du protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) un cadre d'authentification qui prend en charge de multiples mécanismes d'authentification. Dans le schéma proposé, le serveur d'accès réseau (NAS, *Network Access Server*) transmet les paquets EAP de et vers le serveur RADIUS, encapsulés dans les attributs EAP-Message. Ceci présente l'avantage de permettre au NAS de prendre en charge toute méthode d'authentification EAP, sans qu'il soit besoin de code spécifique de la méthode, qui réside sur le serveur RADIUS. Bien que EAP ait été à l'origine développé pour être utilisé avec PPP, il est maintenant aussi utilisé avec IEEE 802.

Le présent document met à jour la RFC 2869.

Table des matières

1. Introduction

Le service d'authentification à distance de l'utilisateur appelant (RADIUS) est un protocole d'authentification, d'autorisation et de comptabilité utilisé pour contrôler l'accès réseau. L'authentification et l'autorisation RADIUS sont spécifiées dans la [RFC2865], et la comptabilité RADIUS est spécifiée dans la [RFC2866] ; RADIUS sur IPv6 est spécifié dans la [RFC3162].

Le protocole d'authentification extensible (EAP) défini dans la [RFC2284], est un cadre d'authentification qui prend en charge de multiples mécanismes d'authentification. EAP peut être utilisé sur des liaisons dédiées, des circuits commutés, et des liaisons filaires aussi bien que sans fil.

Aujourd'hui, EAP a été mis en œuvre avec des hôtes et routeurs qui se connectent via des circuits commutés ou des lignes à numérotage en utilisant PPP [RFC1661]. Il a aussi été mis en œuvre avec des ponts qui prennent en charge [IEEE802]. L'encapsulation EAP sur des supports filaires IEEE 802 est décrite dans [IEEE8021X].

Les attributs RADIUS sont composés de triplets Type-Longueur-Valeur de longueur variable. De nouvelles valeurs d'attributs peuvent être ajoutées sans perturber les mises en œuvre existantes du protocole. La présente spécification décrit les attributs RADIUS qui prennent en charge le protocole d'authentification extensible (EAP) : EAP-Message et Message-Authenticator. Ces attributs ont maintenant une large expérience d'utilisation. L'objet de ce document est de fournir des précisions et de résoudre les problèmes d'interopérabilité.

Comme noté dans la [RFC2865], un serveur d'accès réseau (NAS, *Network Access Server*) qui ne met pas en œuvre un certain service NE DOIT PAS mettre en œuvre les attributs RADIUS pour ce service. Cela implique qu'un NAS qui n'est pas capable d'offrir le service EAP NE DOIT PAS mettre en œuvre les attributs RADIUS pour EAP. Un NAS DOIT traiter un Access-Accept RADIUS demandant un service indisponible comme un Access-Reject.

1.1 Spécification des exigences

Dans le présent document, plusieurs mots sont utilisés pour signifier les exigences de la spécification. Ces mots sont souvent en majuscules. Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans la [RFC2119].

1.2 Terminologie

Le présent document utilise fréquemment les termes suivants :

authentificateur : extrémité de la liaison qui requiert l'authentification. Aussi appelé le serveur d'accès réseau (NAS) ou le client RADIUS. Dans la terminologie IEEE 802.1X, le terme authentificateur est utilisé.

homologue : l'autre extrémité de la liaison point à point, du segment de LAN point à point (IEEE 802.1X) ou de la liaisons sans fil, qui est authentifié par l'authentificateur. Dans IEEE 802.1X, cette extrémité est appelée le solliciteur.

serveur d'authentification : un serveur d'authentification est une entité qui fournit un service d'authentification à un authentificateur (NAS). Ce service vérifie, à partir des accréditifs fournis par l'homologue, la revendication d'identité faite par l'homologue ; il peut aussi fournir des accréditifs permettant à l'homologue de vérifier l'identité du serveur d'authentification. Dans le présent document, il est supposé que le NAS opère comme un intermédiaire, transmettant les paquets EAP entre le serveur RADIUS et l'homologue EAP. Donc le serveur RADIUS opère comme un serveur d'authentification.

éliminer en silence : cela signifie que la mise en œuvre élimine le paquet sans autre traitement. La mise en œuvre DEVRAIT fournir la capacité d'enregistrer l'erreur, incluant le contenu du paquet éliminé en silence, et DEVRAIT enregistrer l'événement dans un compteur de statistiques.

message affichable : ceci est interprété comme étant une chaîne de caractères lisibles par l'homme, et NE DOIT PAS affecter le fonctionnement du protocole. Le codage du message DOIT respecter le format de transformation UTF-8 [RFC2279].

serveur d'accès réseau (NAS, *Network Access Server*) : c'est l'appareil qui fournit l'accès au réseau. Aussi appelé l'authentificateur (terminologie IEEE 802.1X ou EAP) ou le client RADIUS.

service : le NAS fournit un service à l'utilisateur, comme IEEE 802 ou PPP.

session : chaque service fourni par le NAS à un homologue constitue une session, avec le début de la session défini comme le point où le service est fourni en premier et la fin de la session définie comme le point où le service se termine. Un homologue peut avoir de multiples sessions en parallèle ou en série si le NAS le prend en charge, avec chaque session générant un début et un arrêt séparés de l'enregistrement comptable.

2. Prise en charge d'EAP par RADIUS

Le protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) décrit dans la [RFC2284], fournit un mécanisme standard pour prendre en charge des méthodes d'authentification supplémentaires sans que le NAS soit mis à niveau pour prendre en charge chaque nouvelle méthode. Grâce à l'utilisation de EAP, la prise en charge d'un certain nombre de schémas d'authentification peut être ajoutée, incluant des cartes à mémoire, Kerberos [RFC1510], la clé publique [RFC2716], les mots de passe à usage unique [RFC2284], et d'autres.

Un des avantages de l'architecture EAP est sa souplesse. EAP est utilisé pour choisir un mécanisme d'authentification spécifique. Plutôt que d'exiger que le NAS soit mis à jour pour prendre en charge chaque nouvelle méthode d'authentification, EAP permet d'utiliser un serveur d'authentification mettant en œuvre des méthodes d'authentification, le NAS agissant comme intermédiaire pour certaines ou toutes les méthodes et homologues.

Un NAS PEUT authentifier les homologues locaux tout en agissant en même temps comme intermédiaire pour des homologues non locaux et les méthodes d'authentification qu'il ne met pas en œuvre localement. Un NAS qui met en œuvre la présente spécification n'est pas obligé d'utiliser RADIUS pour authentifier chaque homologue. Cependant, une fois que le NAS a commencé d'agir comme intermédiaire pour une certaine session, il ne peut plus effectuer l'authentification locale pour cette session.

Afin de prendre en charge EAP au sein de RADIUS, deux nouveaux attributs, EAP-Message et Message-Authenticator, sont introduits par le présent document. Cette Section décrit comment ces nouveaux attributs peuvent être utilisés pour fournir la prise en charge de EAP au sein de RADIUS.

2.1 Vue d'ensemble du protocole

Dans RADIUS/EAP, RADIUS est utilisé pour faire la navette des paquets EAP encapsulés dans RADIUS entre le NAS et un serveur d'authentification.

L'homologue qui s'authentifie et le NAS commencent la conversation EAP en négociant l'utilisation de EAP. Une fois que EAP a été négocié, le NAS DEVRAIT envoyer un message de demande EAP initiale à l'homologue qui s'authentifie. Cela va normalement être un EAP-Request/Identity, bien que ce pourrait être un EAP-Request pour une méthode d'authentification (types 4 et au dessus). Un NAS PEUT être configuré à s'initier avec une méthode d'authentification par défaut. Ceci est utile dans des cas où l'identité est déterminée par d'autres moyens (comme Called-Station-Id, Calling-Station-Id et/ou Originating-Line-Info) lorsque une seule méthode d'authentification est requise, qui inclut son propre échange d'identité, lorsque il est désiré que l'identité soit cachée, de sorte que l'identité n'est pas demandée tant qu'un canal protégé n'a pas été établi.

L'homologue réplique avec une EAP-Response. Le NAS PEUT déterminer à partir de la réponse qu'il devrait procéder à l'authentification locale. Autrement, le NAS PEUT agir comme intermédiaire, encapsulant la réponse EAP au sein d'un attribut EAP-Message envoyé au serveur RADIUS dans un paquet RADIUS Access-Request. Si le NAS envoie un message EAP-Request/Identity comme paquet initial, l'homologue répond avec un EAP-Response/Identity. Le NAS peut déterminer que l'homologue est local et procéder à l'authentification locale. Si aucune correspondance n'est trouvée dans la liste des utilisateurs locaux, le NAS encapsule le message EAP-Response/Identity dans un attribut EAP-Message, inclus dans un paquet Access-Request.

À réception d'un paquet Access-Request valide contenant un ou des attributs EAP-Message, un serveur RADIUS conforme à la présente spécification et souhaitant s'authentifier avec EAP DOIT répondre avec un paquet Access-Challenge

contenant un ou des attributs EAP-Message. Si le serveur RADIUS ne prend pas en charge EAP ou ne souhaite pas s'authentifier avec EAP, il DOIT répondre avec un Access-Reject.

Le ou les attributs EAP-Message encapsulent un seul paquet EAP que le NAS désencapsule et passe à l'homologue qui s'authentifie. L'homologue répond alors avec un paquet EAP-Response que le NAS encapsule dans une Access-Request contenant un ou des attributs EAP-Message. EAP est un protocole "verrouillé", de sorte qu'à part la demande initiale, une nouvelle demande ne peut pas être envoyée avant de recevoir une réponse valide.

La conversation continue jusqu'à ce qu'un paquet Access-Reject ou Access-Accept soit reçu du serveur RADIUS. La réception d'un paquet RADIUS Access-Reject DOIT résulter en le refus par le NAS de l'accès à l'homologue qui s'authentifie. Un paquet RADIUS Access-Accept termine avec succès la phase d'authentification. Le NAS NE DOIT PAS "fabriquer" un paquet de succès ou d'échec en résultat d'une fin de temporisation. Après l'écoulement d'un nombre convenable de fins de temporisation, le NAS DEVRAIT plutôt terminer la conversation EAP.

En utilisant RADIUS, le NAS peut agir comme intermédiaire pour une conversation EAP entre l'homologue et le serveur d'authentification, sans avoir besoin de mettre en œuvre la méthode EAP utilisée entre eux. Lorsque le NAS initie la conversation en envoyant une EAP-Request pour une méthode d'authentification, il peut n'être pas obligé que le NAS mette pleinement en œuvre la méthode EAP reflétée dans la demande EAP initiale. Selon la méthode initiale, il peut être suffisant que le NAS soit configuré avec le paquet initial à envoyer à l'homologue, et que le NAS agisse comme intermédiaire pour les messages suivants. Noter que comme le NAS encapsule seulement la réponse EAP dans sa demande d'accès initiale, la demande EAP initiale dans la méthode d'authentification n'est pas disponible au serveur RADIUS. Pour que le serveur RADIUS soit capable de continuer la conversation, soit la demande EAP initiale est résiduelle, de sorte que le serveur RADIUS n'a pas besoin de la connaître, soit les informations pertinentes provenant de la demande EAP initiale (comme un nom occasionnel) sont reflétées dans la réponse EAP initiale, de sorte que le serveur RADIUS peut les obtenir sans avoir reçu la demande EAP initiale.

Lorsque la demande EAP initiale envoyée par le NAS est pour un type d'authentification (4 ou supérieur) l'homologue PEUT répondre avec un NAK indiquant qu'il préférerait une autre méthode d'authentification qui n'est pas mise en œuvre localement. Dans ce cas, le NAS DEVRAIT envoyer une Access-Request encapsulant la réponse/NAK EAP reçue. Cela donne au serveur RADIUS une indication sur la ou les méthodes d'authentification préférées par l'homologue, bien que cela ne donne pas d'informations sur le type de la demande d'origine. Cela donne aussi au serveur l'identifiant utilisé dans la demande EAP initiale, de sorte que les conflits d'identifiant peuvent être évités.

Afin d'évaluer si les solutions préférées par l'homologue qui s'authentifie sont permises, le serveur RADIUS va normalement répondre avec un Access-Challenge contenant le ou les attributs du message EAP qui encapsule une demande/identité EAP (type 1). Cela permet au serveur RADIUS de déterminer l'identité de l'homologue, afin d'être capable de restituer la politique d'authentification associée. Autrement, une demande EAP pour une méthode d'authentification (type 4 ou supérieure) pourrait être envoyée. Comme le serveur RADIUS peut n'avoir pas connaissance du type de la demande EAP initiale, il est possible au serveur RADIUS de choisir une méthode inacceptable, et à l'homologue de répondre avec un autre NAK

Afin de permettre à des mandataires RADIUS sans capacité EAP de transmettre le paquet Access-Request, si le NAS envoie initialement un message EAP-Request/Identity à l'homologue, le NAS DOIT copier le contenu du champ Type-Data de la EAP-Response/Identity reçue de l'homologue dans l'attribut User-Name et DOIT inclure le champ Type-Data de la EAP-Response/Identity dans l'attribut User-Name dans chaque Access-Request suivante. Comme les mandataires RADIUS sont supposés agir comme intermédiaires, on ne peut pas s'attendre à ce qu'ils analysent une EAP-Response/Identity encapsulée dans un ou des attributs EAP-Message. Si le NAS envoie initialement une EAP-Request pour une méthode d'authentification, et si l'identité de l'homologue ne peut pas être déterminée à partir de la réponse EAP, alors l'attribut User-Name DEVRAIT être déterminé par d'autres moyens. Comme noté dans la [RFC2865] paragraphe 5.6, il est recommandé que les demandes d'accès utilisent la valeur de Calling-Station-Id comme valeur de l'attribut User-Name.

Il y a un certain nombre d'avantages à ce que le NAS envoie le paquet Demande EAP initial :

1. Cela économise un aller-retour entre le NAS et le serveur RADIUS.

2. Une demande d'accès est seulement envoyée au serveur RADIUS si l'homologue qui s'authentifie envoie une réponse EAP, confirmant qu'il prend en charge EAP. Dans des situations où les homologues peuvent être sans capacité EAP, initier une demande d'accès RADIUS sur une indication "sens de porteuse" ou "support actif" peut résulter en de nombreux échanges d'authentification qui ne peuvent pas s'achever sur un succès. Par exemple, sur les réseaux filaires [IEEE8021X] les demandeurs n'initient normalement pas la conversation 802.1X avec un EAPOL-Start. Donc un pont à capacité IEEE 802.1X peut n'être pas capable de déterminer si l'homologue prend en charge EAP avant d'avoir reçu une

réponse à la demande EAP initiale.

3. Cela permet que certains homologues soient authentifiés en local.

Bien que l'envoi par le NAS du paquet Demande EAP initiale ait de substantiels avantages, cette technique ne peut pas être universellement employée. Il y a des circonstances dans lesquelles l'identité de l'homologue est déjà connue (comme quand l'authentification et la comptabilité sont traitées sur la base de Called-Station-Id, Calling-Station-Id et/ou Originating-Line-Info) mais où la méthode EAP appropriée peut varier en fonction de cette identité.

Plutôt que d'envoyer un paquet Demande EAP initial à l'homologue qui s'authentifie, à la détection de la présence de l'homologue, le NAS PEUT envoyer un paquet Demande d'accès au serveur RADIUS contenant un attribut EAP-Message signifiant EAP-Start. Le serveur RADIUS va normalement répondre avec un Access-Challenge contenant un ou des attributs EAP-Message encapsulant une EAP-Request/Identity (type 1). Cependant, une EAP-Request pour une méthode d'authentification (type 4 ou supérieur) peut aussi être envoyée par le serveur.

EAP-Start est indiqué par l'envoi d'un attribut EAP-Message avec une longueur de 2 (pas de données). Le Calling-Station-Id DEVRAIT être inclus dans l'attribut User-Name. Il peut en résulter l'envoi d'une demande d'accès RADIUS par le NAS au serveur RADIUS sans que soit d'abord confirmé que l'homologue prend en charge EAP. Comme cette technique peut résulter en un grand nombre de conversations RADIUS non achevées, dans les situations où des homologues sans capacité EAP sont courants, ou où la prise en charge d'EAP par les homologues ne peut pas être déterminée au contact initial (par exemple [IEEE8021X] les demandeurs qui n'initient pas la conversation avec un EAPOL-Start) elle NE DEVRAIT PAS être employée par défaut.

Pour les demandes RADIUS relayées par un mandataire, il y a deux méthodes de traitement. Si le domaine est déterminé sur la base de Calling-Station-Id, Called-Station-Id et/ou Originating-Line-Info, le serveur RADIUS peut relayer le Access-Request/EAP-Start RADIUS initial. Si le domaine est déterminé sur la base de l'identité de l'homologue, le serveur RADIUS local DOIT répondre avec un Access-Challenge RADIUS incluant un attribut EAP-Message encapsulant un paquet EAP-Request/Identity. La réponse de l'homologue qui s'authentifie DEVRAIT être relayée par un mandataire au serveur d'authentification final.

Si une demande d'accès est envoyée à un serveur RADIUS qui ne prend pas en charge l'attribut EAP-Message, un Access-Reject DOIT alors être envoyé en réponse. À réception d'un Access-Reject, le NAS DOIT refuser l'accès à l'homologue qui s'authentifie.

2.2 Paquets invalides

Lorsque il agit comme intermédiaire, le NAS DOIT valider les champs d'en-tête EAP (Code, Identifiant, Longueur) avant de transmettre un paquet EAP au ou du serveur RADIUS. À réception d'un paquet EAP de l'homologue, le NAS vérifie les champs Code (2) et Longueur, et confronte la valeur de l'identifiant à l'identifiant en cours, fourni par le serveur RADIUS dans la demande EAP la plus récemment validée. À réception d'un paquet EAP du serveur RADIUS (encapsulé dans un Access-Challenge) le NAS vérifie les champs Code (1) et Longueur, puis met à jour la valeur d'identifiant courante. Les réponses EAP en cours qui ne correspondent pas à la valeur d'identifiant courante sont éliminées en silence par le NAS.

Comme les champs de méthode EAP (Type, Type-Data) ne sont normalement pas validés par un NAS qui opère comme intermédiaire, en dépit de ces vérifications, il est possible qu'un NAS transmette un paquet EAP invalide au ou du serveur RADIUS. Un serveur RADIUS qui reçoit un ou des attributs EAP-Message qu'il ne comprend pas DEVRAIT déterminer si l'erreur est fatale ou non sur la base du type EAP. Un serveur RADIUS qui détermine qu'une erreur fatale s'est produite DOIT envoyer un Access-Reject contenant un attribut EAP-Message encapsulant un EAP-Failure.

Un serveur RADIUS qui détermine qu'une erreur non fatale s'est produite PEUT envoyer un Access-Challenge au NAS incluant un ou des attributs EAP-Message ainsi qu'un attribut Error-Cause [RFC3576] avec la valeur 202 (en décimal) "Paquet EAP invalide (ignoré)". Le Access-Challenge DEVRAIT encapsuler dans un ou des attributs EAP-Message le paquet Demande EAP le plus récemment envoyé (incluant la même valeur d'identifiant). À réception d'un tel Access-Challenge, un NAS qui met en œuvre une version antérieure de la présente spécification va désencapsuler la demande EAP et l'envoyer à l'homologue, qui va retransmettre la réponse EAP.

Un NAS conforme à la présente spécification, à réception d'un Access-Challenge avec un attribut Error-Cause de valeur 202 (décimal) DEVRAIT éliminer le paquet Réponse EAP le plus récemment transmis au serveur RADIUS et vérifier si des paquets Réponse EAP supplémentaires ont été reçus qui correspondent à la valeur courante d'identifiant. Si il en est, un nouveau paquet Réponse EAP, si disponible, DOIT être envoyé au serveur RADIUS dans une demande d'accès, et le ou les

attributs EAP-Message inclus dans le Access-Challenge sont éliminés en silence. Si aucun paquet Réponse EAP n'est disponible, alors la demande EAP encapsulée dans le Access-Challenge est envoyée à l'homologue, et le temporisateur de retransmission est remis à zéro.

Afin d'assurer la protection contre les attaques de déni de service (DoS) il est conseillé que le NAS alloue une mémoire tampon finie pour les paquets EAP reçus de l'homologue, et élimine les paquets selon une politique appropriée une fois que la mémoire tampon est remplie. Aussi, il est conseillé que le serveur RADIUS permette seulement un nombre modeste de paquets EAP invalides dans une seule session, avant de terminer la session avec un Access-Reject. Par défaut, une valeur de 5 paquets EAP invalides est recommandée.

2.3 Retransmission

Comme noté dans la [RFC2284], si un paquet EAP est perdu dans le transit entre l'homologue qui s'authentifie et le NAS (ou vice versa) le NAS va retransmettre.

Il peut être nécessaire d'ajuster dans certains cas les stratégies de retransmission et les temporisations d'authentification. Par exemple, quand une carte à jeton est utilisée, du temps supplémentaire peut être nécessaire pour permettre à l'utilisateur de trouver la carte et entrer le jeton. Comme le NAS ne va normalement pas avoir connaissance des paramètres requis, ils doivent être fournis par le serveur RADIUS. Ceci peut être réalisé par l'inclusion de l'attribut Session-Timeout au sein du paquet Access-Challenge.

Si Session-Timeout est présent dans un paquet Access-Challenge qui contient aussi un message EAP, la valeur de Session-Timeout est utilisée pour régler le temporisateur de retransmission EAP pour cette demande EAP, et seulement celle là. Une fois la demande EAP envoyée, le NAS lance le temporisateur de retransmission, et si il expire sans qu'il ait reçu une réponse EAP correspondant à la demande, la demande EAP est retransmise.

2.4 Fragmentation

En utilisant l'attribut EAP-Message, il est possible que le serveur RADIUS encapsule un paquet EAP qui est plus grand que la MTU sur la liaison entre le NAS et l'homologue. Comme il n'est pas possible au serveur RADIUS d'utiliser la découverte de MTU pour s'assurer de la MTU de la liaison, l'attribut Framed-MTU peut être inclus dans un paquet Access-Request contenant un attribut EAP-Message afin de fournir cette information au serveur RADIUS. Un serveur RADIUS qui a reçu un attribut Framed-MTU dans un paquet Access-Request NE DOIT PAS envoyer d'autre paquet dans cette conversation EAP contenant des attributs EAP-Message dont les valeurs, enchaînées, excèdent la longueur spécifiée par la valeur de Framed-MTU, en prenant en compte le type de liaison (spécifié par l'attribut NAS-Port-Type). Par exemple, comme noté au paragraphe 3.10 de la [RFC3580], pour une valeur de NAS-Port-Type de IEEE 802.11, le serveur RADIUS peut envoyer un paquet EAP de Framed-MTU moins quatre (4) octets, en prenant en compte les frais généraux supplémentaires pour les champs IEEE 802.1X Version (1), Type (1) et Longueur de corps (2).

2.5 Autres utilisations

Actuellement, la conversation entre les serveurs de sécurité et le serveur RADIUS est souvent propriétaire à cause du manque de normalisation. Afin d'augmenter la normalisation et assurer l'interopérabilité entre les fournisseurs RADIUS et les fournisseurs de solutions de sécurité, il est recommandé que EAP encapsulé dans RADIUS soit utilisé pour cette conversation.

Cela présente l'avantage de permettre au serveur RADIUS de prendre en charge EAP sans avoir besoin de code spécifique de l'authentification au sein du serveur RADIUS. Le code spécifique de l'authentification peut alors résider plutôt sur un serveur de sécurité.

Dans le cas où EAP encapsulé dans RADIUS est utilisé dans une conversation entre un serveur RADIUS et un serveur de sécurité, le serveur de sécurité va normalement retourner un message Access-Accept sans inclure les attributs attendus couramment retournés dans un Access-Accept. Cela signifie que le serveur RADIUS DOIT ajouter ces attributs avant d'envoyer un message Access-Accept au NAS.

2.6 Lignes directrices pour l'utilisation

2.6.1 Espace d'identifiant

Dans EAP, chaque session a son propre espace d'identifiant unique. Les mises en œuvre de serveur RADIUS DOIVENT être capables de distinguer entre paquets EAP avec le même identifiant existant au sein de sessions distinctes, provenant du même NAS. À cette fin, les sessions peuvent être distinguées sur la base du NAS et des attributs d'identification de session. Les attributs d'identification de NAS incluent NAS-Identifier, NAS-IPv6-Address et NAS-IPv4-Address. Les attributs d'identification de session incluent User-Name, NAS-Port, NAS-Port-Type, NAS-Port-Id, Called-Station-Id, Calling-Station-Id et Originating-Line-Info.

2.6.2 Inversion de rôle

Comme EAP est un protocole d'homologue à homologue, une authentification indépendante et simultanée peut avoir lieu dans la direction inverse. Les deux homologues peuvent agir comme authentificateurs et authentifiés en même temps.

Cependant, l'inversion de rôle n'est pas prise en charge par la présente spécification. Un serveur RADIUS DOIT répondre à une Access-Request encapsulant une EAP-Request avec un Access-Reject. Afin d'éviter des retransmissions par l'homologue, le Access-Reject DEVRAIT inclure un paquet EAP-Response/NAK n'indiquant pas de méthode préférée, encapsulé dans un ou des attributs EAP-Message

2.6.3 Conflit de messages

Le NAS DOIT prendre ses décisions de contrôle d'accès sur la seule base du type de paquet RADIUS (Access-Accept/Access-Reject). La décision de contrôle d'accès NE DOIT PAS être fondée sur le contenu du paquet EAP encapsulé dans un ou plusieurs attributs EAP-Message, si il en est de présents.

Les paquets Access-Accept DEVRAIENT avoir seulement un attribut EAP-Message, contenant EAP Success ; de même, les paquets Access-Reject DEVRAIENT avoir seulement un attribut EAP-Message, contenant EAP Failure.

Lorsque le paquet EAP encapsule ne correspond pas au résultat impliqué par le type de paquet RADIUS, la combinaison va probablement causer une certaine confusion, parce que le NAS et l'homologue vont arriver à des conclusions différentes sur le résultat de l'authentification.

Par exemple, si le NAS reçoit un Access-Reject avec un succès EAP encapsulé, il ne va pas accorder l'accès à l'homologue. Cependant, à réception du succès EAP, l'homologue va être conduit à croire qu'il a réussi à s'authentifier.

Si le NAS reçoit un Access-Accept avec un échec EAP encapsulé, il va accorder l'accès à l'homologue. Cependant, en recevant un échec EAP, l'homologue va être amené à croire que son authentification a échoué. Si aucun attribut EAP-Message n'est inclus dans un Access-Accept ou Access-Reject, l'homologue peut n'être pas informé du résultat de l'authentification, alors que le NAS va effectuer une action pour permettre ou refuser l'accès.

Comme décrit dans la [RFC2284], les paquets Succès et Échec EAP n'ont pas d'accusé de réception, et ces paquets terminent la conversation EAP. Par suite, si ces paquets sont encapsulés dans un Access-Challenge, aucune réponse ne va être reçue, et donc le NAS ne va pas envoyer d'autre Access-Request au serveur RADIUS pour la session. Il en résulte que le serveur RADIUS ne va pas indiquer au NAS si il faut permettre ou refuser l'accès, alors que l'homologue va être informé du résultat de l'authentification.

Pour éviter ces conflits, les combinaisons suivantes NE DEVRAIENT PAS être envoyées par un serveur RADIUS :
Access-Accept/EAP-Message/Échec EAP
Access-Accept/pas d'attribut EAP-Message
Access-Accept/EAP-Start
Access-Reject/EAP-Message/Réussite EAP
Access-Reject/pas d'attribut EAP-Message
Access-Reject/EAP-Start
Access-Challenge/EAP-Message/Réussite EAP
Access-Challenge/EAP-Message/Échec EAP
Access-Challenge/pas d'attribut EAP-Message
Access-Challenge/EAP-Start

Comme la responsabilité d'éviter les conflits incombe au serveur RADIUS, le NAS NE DOIT PAS "fabriquer" de paquets

EAP afin de corriger les messages contradictoires qu'il reçoit. Ce comportement, à l'origine obligatoire dans [IEEE8021X], va être déconseillé à l'avenir.

2.6.4 Priorité

Un paquet RADIUS Access-Accept ou Access-Reject peut contenir un ou des attributs EAP-Message. Afin de s'assurer du traitement correct des paquets RADIUS, le NAS DOIT d'abord traiter les attributs, incluant les attributs EAP-Message, avant de traiter l'indication Accept/Reject.

2.6.5 Messages affichables

L'attribut Reply-Message, défini dans la [RFC2865], paragraphe 5.18, indique le texte qui peut être affiché à l'homologue. Ceci est similaire au concept de notification EAP, défini dans la [RFC2284]. Quand il envoie un message affichable au NAS durant une conversation EAP, le serveur RADIUS DOIT encapsuler les messages affichables dans un ou des attributs EAP-Message/EAP-Request/Notification. Les attributs Reply-Message NE DOIVENT PAS être inclus dans un message RADIUS contenant un attribut EAP-Message. Un EAP-Message/EAP-Request/Notification NE DEVRAIT PAS être inclus dans un paquet Access-Accept ou Access-Reject.

Dans certaines mises en œuvre existantes, un NAS qui reçoit un ou des attributs Reply-Message copie les champs Text dans le champ Type-Data d'un paquet EAP-Request/Notification, remplit le champ Identifiant, et envoie cela à l'homologue. Cependant, plusieurs problèmes découlent de cela :

1. Réponses inattendues. À réception d'une EAP-Request/Notification, l'homologue va envoyer une EAP-Response/Notification, et le NAS va passer cela au serveur RADIUS, encapsulé dans un ou des attributs EAP-Message. Cependant, le serveur RADIUS peut ne pas attendre une Access-Request contenant un attribut EAP-Message/EAP-Response/Notification.
   Par exemple, considérons ce qui arrive quand un Reply-Message est inclus dans un paquet Access-Accept ou Access-Reject sans attribut EAP-Message présent. Si la valeur de l'attribut Reply-Message est copiée dans le Type-Data d'une EAP-Request/Notification et est envoyée à l'homologue, il va en résulter une Access-Request contenant un attribut EAP-Message/EAP-Response/Notification envoyé par le NAS au serveur RADIUS. Comme un paquet Access-Accept ou Access-Reject termine la conversation RADIUS RADIUS, une telle Access-Request ne serait pas attendue, et pourrait être interprétée comme le début d'une autre conversation.

2. Conflits d'identifiant. Alors que la EAP-Request/Notification est un paquet EAP contenant un champ Identifiant, l'attribut Reply-Message ne contient pas de champ Identifiant. Par suite, un NAS qui reçoit un attribut Reply-Message et qui souhaite le traduire en une EAP-Request/Notification va devoir choisir une valeur d'identifiant. Il est possible que la valeur d'identifiant choisie soit en conflit avec une valeur choisie par le serveur RADIUS pour un autre paquet dans la conversation EAP, causant potentiellement une confusion entre un nouveau paquet et une retransmission.

Pour éviter ces problèmes, un NAS qui reçoit un attribut Reply-Message du serveur RADIUS DEVRAIT éliminer en silence l'attribut, plutôt que de tenter de le traduire en une demande de notification EAP.

3. Attributs

Les attributs NAS-Port ou NAS-Port-Id DEVRAIENT être inclus par le NAS dans les paquets Access-Request, et les attributs NAS-Identifier, NAS-IP-Address ou NAS-IPv6-Address DOIVENT être inclus. Afin de permettre la transmission de l'Access-Reply par des mandataires sans capacité EAP, si un attribut User-Name a été inclus dans une Access-Request, le serveur RADIUS DOIT inclure l'attribut User-Name dans les paquets Access-Accept suivants. Sans l'attribut User-Name, la comptabilité et la facturation deviennent difficiles à gérer. L'attribut User-Name au sein du paquet Access-Accept n'a pas besoin d'être le même que l'attribut User-Name dans la Access-Request.

3.1 EAP-Message

Description : cet attribut encapsule les paquets EAP [RFC2284] de façon à permettre au NAS d'authentifier les homologues via EAP sans avoir à comprendre la méthode EAP par laquelle ils passent.

Le NAS place les messages EAP reçus de l'homologue qui s'authentifie dans un ou plusieurs attributs EAP-Message et les transmet au serveur RADIUS dans un message Access-Request. Si plusieurs attributs EAP-Message sont contenus dans un

paquet Access-Request ou Access-Challenge, ils DOIVENT être dans l'ordre et ils DOIVENT être des attributs consécutifs dans le paquet Access-Request ou Access-Challenge. Le serveur RADIUS peut retourner les attributs EAP-Message dans les paquets Access-Challenge, Access-Accept et Access-Reject.

Quand RADIUS est utilisé pour permettre l'authentification EAP, les paquets Access-Request, Access-Challenge, Access-Accept, et Access-Reject DEVRAIENT contenir un ou plusieurs attributs EAP-Message. Lorsque plus d'un attribut EAP-Message est inclus, il est supposé que les attributs sont enchaînés pour former un seul paquet EAP.

Plusieurs paquets EAP NE DOIVENT PAS être codés dans les attributs EAP-Message contenus dans un seul paquet Access-Challenge, Access-Accept, Access-Reject ou Access-Request.

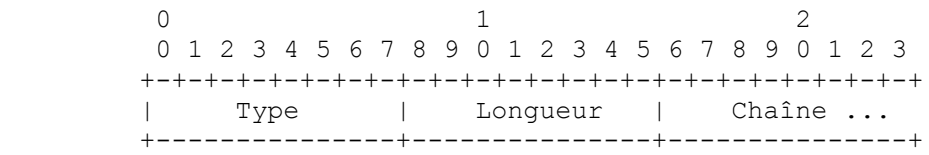
On s'attend à ce que EAP va être utilisé pour mettre en œuvre diverses méthodes d'authentification, incluant des méthodes qui impliquent une cryptographie forte. Afin d'empêcher des attaquants de subvertir EAP en attaquant RADIUS/EAP, (par exemple, en modifiant les paquets Réussite EAP ou Échec EAP) il est nécessaire que RADIUS assure l'authentification et la protection d'intégrité par paquet.

Donc l'attribut Message-Authenticator DOIT être utilisé pour protéger tous les paquets Access-Request, Access-Challenge, Access-Accept, et Access-Reject contenant un attribut EAP-Message.

Les paquets Access-Request incluant un ou des attributs EAP-Message sans un attribut Message-Authenticator DEVRAIENT être éliminés en silence par le serveur RADIUS. Un serveur RADIUS qui prend en charge l'attribut EAP-Message DOIT calculer la valeur correcte de Message-Authenticator et DOIT éliminer en silence le paquet si il ne correspond pas à la valeur envoyée. Un serveur RADIUS qui ne prend pas en charge l'attribut EAP-Message DOIT retourner un Access-Reject si il reçoit une Access-Request contenant un attribut EAP-Message.

Les paquets Access-Challenge, Access-Accept, ou Access-Reject qui incluent un ou des attributs EAP-Message sans un attribut Message-Authenticator DEVRAIENT être éliminés en silence par le NAS. Un NAS qui prend en charge l'attribut EAP-Message DOIT calculer la valeur correcte de Message-Authenticator et DOIT éliminer en silence le paquet si il ne correspond pas à la valeur envoyéé.

Un résumé du format de l'attribut EAP-Message est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 79 pour EAP-Message

Longueur : ≤ 3

Chaîne : le champ Chaîne contient un paquet EAP, comme défini dans la [RFC2284]. Si plusieurs attributs EAP-Message sont présents dans un paquet, leurs valeurs devraient être enchaînées ; cela permet que les paquets EAP de plus de 253 octets soient transportés par RADIUS.

3.2 Message-Authenticator

Description : cet attribut PEUT être utilisé pour authentifier et protéger en intégrité les demandes d'accès afin d'empêcher l'usurpation d'identité. Il PEUT être utilisé dans toute demande d'accès. Il DOIT être utilisé dans toute Access-Request, Access-Accept, Access-Reject ou Access-Challenge qui inclut un attribut EAP-Message.

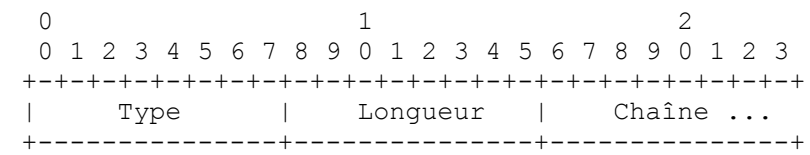
Un serveur RADIUS recevant une Access-Request avec un attribut Message-Authenticator présent DOIT calculer la valeur correcte du Message-Authenticator et éliminer en silence le paquet si il ne correspond pas à la valeur envoyée.

Un client RADIUS recevant un Access-Accept, Access-Reject ou Access-Challenge avec un attribut Message-Authenticator présent DOIT calculer la valeur correcte du Message-Authenticator et éliminer en silence le paquet si il ne correspond pas à la valeur envoyée.

Cet attribut n'est pas exigé dans les demandes d'accès qui incluent l'attribut User-Password, mais est utile pour empêcher

des attaques contre d'autres types d'authentification. Cet attribut est destiné à déjouer les tentatives d'établissement d'un NAS "félon" par un attaquant, et d'effectuer des attaques de dictionnaire en ligne contre le serveur RADIUS. Il n'offre pas de protection contre les attaques "hors ligne" où l'attaquant intercepte les paquets qui contiennent (par exemple) les défis et réponses CHAP, et effectue une attaque de dictionnaire hors ligne contre ces paquets.

Un résumé du format de l'attribut Message-Authenticator est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 80 pour Message-Authenticator

Longueur : 18

Chaîne : lorsque il est présent dans un paquet Access-Request, Message-Authenticator est un hachage HMAC-MD5 [RFC2104] du paquet Access-Request entier, incluant les champs Type, ID, Longueur et Authentificateur, en utilisant le secret partagé comme clé, comme suit .

Message-Authenticator = HMAC-MD5 (Type, Identifiant, Longueur, Authentifiant de demande, Attributs)

Quand la vérification d'intégrité de message est calculée, la chaîne de signature devrait être considérée comme étant seize octets de zéros.

Pour les paquets Access-Challenge, Access-Accept, et Access-Reject, le Message-Authenticator est calculé comme suit, en utilisant le Request-Authenticator provenant de la demande d'accès auquel ce paquet est en réponse :

Message-Authenticator = HMAC-MD5 (Type, Identifiant, Longueur, Request Authenticator, Attributs)

Quand la vérification d'intégrité de message est calculée, la chaîne de signature devrait être considérée comme étant seize octets de zéros. Le secret partagé est utilisé comme clé pour la vérification d'intégrité du message HMAC-MD5. Le Message-Authenticator est calculé et inséré dans le paquet avant le calcul de la Response-Authenticator.

3.3 Tableau des attributs

Le tableau qui suit donne des indications sur les attributs qui peuvent être trouvés dans les paquets incluant le ou les attributs EAP-Message, et en quelle quantité. Les attributs EAP-Message et Message-Authenticator spécifiés dans le présent document NE DOIVENT PAS être présents dans une Accounting-Request. Si une entrée de tableau est omise, les valeurs qui se trouvent dans les [RFC2548], [RFC2865], [RFC2868], [RFC2869] et [RFC3162] devraient être supposées.

Demande	Accept	Reject	Challenge	n°	Attribut
0-1	0-1	0	0	1	User-Name
0	0	0	0	2	User-Password [Note 1]
0	0	0	0	3	CHAP-Password [Note 1]
0	0	0	0	18	Reply-Message
0	0	0	0	60	CHAP-Challenge
0	0	0	0	70	ARAP-Password [Note 1]
0	0	0	0	75	Password-Retry
1+	1+	1+	1+	79	EAP-Message [Note 1]
1	1	1	1	80	Message-Authenticator [Note 1]
0-1	0	0	0	94	Originating-Line-Info [Note 3]
0	0	0-1	0-1	101	Error-Cause [Note 2]

[Note 1] Une demande d'accès qui contient un attribut User-Password ou CHAP-Password ou ARAP-Password ou un ou plusieurs EAP-Message NE DOIT PAS contenir plus d'un type de ces quatre attributs. Si elle ne contient pas un de ces quatre attributs, elle DEVRAIT contenir un Message-Authenticator. Si un type de paquet contient un attribut EAP-Message, il DOIT aussi contenir un Message-Authenticator. Un serveur RADIUS recevant une Access-

Request ne contenant aucun de ces quatre attributs et ne contenant aussi pas d'attribut Message-Authenticator DEVRAIT l'éliminer en silence.

[Note 2] L'attribut Error-Cause est défini dans la [RFC3576].

[Note 3] L'attribut Originating-Line-Info est défini dans la [RFC4005].

Le tableau suivant définit la signification des entrées du tableau.
0 : cet attribut NE DOIT PAS être présent.
0+ : zéro, une ou plusieurs instances de cet attribut PEUVENT être présentes.
0-1 : zéro ou une instance de cet attribut PEUT être présente.
1 : exactement une instance de cet attribut DOIT être présente.
1+ : un ou plusieurs de ces attributs DOIVENT être présents.

4. Considérations sur la sécurité

4.1 Exigences de sécurité

RADIUS/EAP est utilisé afin de fournir l'authentification et l'autorisation de l'accès au réseau. Par suite, les portions RADIUS et EAP de la conversation sont toutes deux des cibles potentielles d'attaque. Les menaces sont discutées dans les [RFC2607], [RFC2865], et [RFC3162]. Des exemples incluent :

1. Un adversaire peut tenter d'acquérir des données et identités confidentielles en espionnant les paquets RADIUS.
2. Un adversaire peut tenter de modifier les paquets contenant des messages RADIUS.
3. Un adversaire peut tenter d'injecter des paquets dans une conversation RADIUS.
4. Un adversaire peut lancer une attaque de dictionnaire contre le secret partagé RADIUS.
5. Un adversaire peut lancer une attaque de texte en clair connu, espérant récupérer le flux de clé correspondant à un Request-Authenticator.
6. Un adversaire peut tenter de répéter un échange RADIUS.
7. Un adversaire peut tenter de perturber la négociation EAP, afin d'affaiblir l'authentification, ou de gagner l'accès aux mots de passe de l'homologue.
8. Un NAS authentifié peut tenter de falsifier les attributs d'identification de NAS ou de session,
9. Un NAS félon (non authentifié) peut tenter de se faire passer pour un NAS légitime.
10. Un attaquant peut tenter d'agir comme agent interposé.

Pour traiter ces menaces, il est nécessaire de prendre en charge la protection de la confidentialité, l'authentification de l'origine des données, la protection de l'intégrité, et la protection contre la répétition paquet par paquet. L'authentification bidirectionnelle entre le client et le serveur RADIUS doit aussi être fournie. Il n'est pas exigé que les identités des clients et serveurs RADIUS restent confidentielles (par exemple, à un espion passif).

4.2 Protocole de sécurité

Pour traiter les faiblesse de sécurité de RADIUS/EAP, les mises en œuvre de la présente spécification DEVRAIENT prendre en charge IPsec [RFC2401] ainsi que IKE [RFC2409] pour la gestion de clés. IPsec ESP [RFC2406] avec une transformation non nulle DEVRAIT être pris en charge, et IPsec ESP avec transformation de chiffrement non nulle et prise en charge de l'authentification DEVRAIT être utilisé pour assurer par paquet la confidentialité, l'authentification, l'intégrité et la protection contre la répétition. IKE DEVRAIT être utilisé pour la gestion de clé.

Dans RADIUS [RFC2865], un secret partagé est utilisé pour cacher les attributs comme User-Password, ainsi que dans le calcul de la réponse d'authentificateur. Dans la comptabilité RADIUS [RFC2866], le secret partagé est utilisé dans le calcul de la demande et la réponse d'authentificateur.

Comme dans RADIUS, un secret partagé est utilisé pour assurer la confidentialité ainsi que la protection de l'intégrité et l'authentification, utiliser seulement IPsec ESP avec une transformation non nulle peut fournir des services de sécurité suffisants pour se substituer à la sécurité de la couche application RADIUS. Donc, lorsque IPsec AH ou ESP nul est utilisé, il va normalement être encore nécessaire de configurer un secret partagé RADIUS.

Lorsque RADIUS fonctionne sur IPsec ESP avec une transformation non nulle, le secret partagé entre le NAS et le serveur RADIUS NE PEUT PAS être configuré. Dans ce cas, un secret partagé de longueur zéro DOIT être supposé. Cependant, un serveur RADIUS qui ne peut pas savoir si le trafic entrant est protégé par IPsec DOIT être configuré avec un secret partagé

RADIUS non nul.

Quand IPsec ESP est utilisé avec RADIUS, l'authentification, l'intégrité et la protection contre la répétition DOIVENT être utilisées par paquet. 3DES-CBC DOIT être pris en charge comme transformation de chiffrement et AES-CBC DEVRAIT être pris en charge. AES-CBC DEVRAIT être offert comme transformation de chiffrement préférée, si il est pris en charge. HMAC-SHA1-96 DOIT être pris en charge comme transformation d'authentification. DES-CBC NE DEVRAIT PAS être utilisé comme transformation de chiffrement.

Une politique IPsec normale pour un client RADIUS à capacité IPsec est "Initier IPsec, de moi à tout accès de destination UDP 1812". Cela cause l'établissement d'une SA IPsec par le client RADIUS avant l'envoi de trafic RADIUS. Si des serveurs RADIUS contactés par le client ne prennent pas en charge IPsec, une politique plus fine sera alors requise : "Initier IPsec, de moi au serveur RADIUS à capacité IPsec, à l'accès de destination UDP 1812".

Pour un serveur RADIUS à capacité IPsec, une politique IPsec normale est "Accepter IPsec, de tous à moi, accès de destination 1812". Cela cause l'acceptation par le serveur RADIUS (mais elle n'est pas exigée) de l'utilisation de IPsec. Il peut n'être pas approprié d'exiger IPsec pour tous les clients RADIUS qui se connectent à un serveur RADIUS à capacité IPsec, car certains clients RADIUS peut ne pas prendre IPsec en charge.

Lorsque IPsec est utilisé pour la sécurité, et qu'aucun secret partagé RADIUS n'est configuré, il est important que le client et le serveur RADIUS effectuent une vérification d'autorisation. Avant de permettre à un hôte d'agir comme client RADIUS, le serveur RADIUS DEVRAIT vérifier si l'hôte est autorisé à fournir l'accès au réseau. De même, avant de permettre à un hôte d'agir comme serveur RADIUS, le client RADIUS DEVRAIT vérifier si l'hôte est autorisé pour ce rôle.

Les serveurs RADIUS peuvent être configurés avec les adresses IP (pour le mode IKE agressif avec clés pré partagées) ou les FQDN (pour l'authentification par certificat) des clients RADIUS. Autrement, si une autorité de certification (CA, *Certification Authority*) séparée existe pour les clients RADIUS, alors le serveur RADIUS peut configurer cette CA comme une ancre de confiance [RFC3280] pour l'utiliser avec IPsec.

De même, les clients RADIUS peuvent être configurés avec les adresses IP (pour le mode IKE agressif avec clés pré partagées) ou les FQDN (pour l'authentification par certificat) des serveurs RADIUS. Autrement, si une CA séparée existe pour les serveurs RADIUS, alors le client RADIUS peut configurer cette CA comme ancre de confiance pour l'utiliser avec IPsec.

Comme, à la différence de SSL/TLS, IKE ne permet pas d'établir de politiques de certificats sur la base de l'accès, les politiques de certificat doivent être appliquées à toutes les utilisations de IPsec sur les clients et serveurs RADIUS. Dans les déploiements de IPsec qui prennent seulement en charge l'authentification de certificat, une station de gestion qui initie une session telnet protégée par IPsec avec le serveur RADIUS va avoir besoin d'obtenir une chaîne de certificats jusqu'à la CA du client RADIUS. Produire un tel certificat peut n'être pas approprié si la station de gestion n'est pas autorisée comme client RADIUS.

Lorsque les clients RADIUS peuvent obtenir leur adresse IP de façon dynamique (comme un point d'accès qui prend en charge DHCP) le mode IKE principal avec clés pré partagées [RFC2409] NE DEVRAIT PAS être utilisé, car cela exige l'utilisation d'une clé pré partagée de groupe ; le mode agressif DEVRAIT plutôt être utilisé. IKEv2, (travail en cours) pourrait traiter cela à l'avenir. Lorsque les adresses de client RADIUS sont allouées de façon statique, le mode agressif ou le mode principal PEUT être utilisé. Avec l'authentification par certificat, le mode principal DEVRAIT être utilisé.

Il faut faire attention avec le choix de charge utile d'identité IKE phase 1 afin de permettre la transposition des identités en clés pré partagées même avec le mode agressif. Lorsque les charges utiles d'identité ID_IPV4_ADDR ou ID_IPV6_ADDR sont utilisées et que les adresses sont allouées dynamiquement, la transposition des identités en clés n'est pas possible, de sorte que des clés de groupe pré partagées sont encore une nécessité pratique. Par suite, la charge utile d'identité ID_FQDN DEVRAIT être employée dans les situations où le mode agressif est utilisé avec des clés pré partagées et où les adresses IP sont allouées de façon dynamique. Cette approche a aussi d'autres avantages, car elle permet au serveur et client RADIUS de se configurer sur la base du nom de domaine pleinement qualifié de leurs homologues.

Noter qu'avec IPsec, les services de sécurité sont négociés à la granularité d'une SA IPsec, de sorte que les échanges RADIUS qui exigent un ensemble de services de sécurité différent de celui négocié avec les SA IPsec existantes vont avoir besoin de négocier une nouvelle SA IPsec. Des SA IPsec séparées sont aussi conseillées lorsque des considérations de qualité de service imposent un traitement différent des conversations RADIUS. Tenter d'appliquer une qualité de service différente aux connexions traitées par la même SA IPsec peut résulter en une réorganisation, et tomber en dehors de la fenêtre de répétition. Pour une discussion de ces questions, voir la [RFC2983].

4.3 Questions de sécurité

Ce paragraphe donne plus de détails sur les vulnérabilités identifiées au paragraphe 4.1., et comment elles peuvent être atténuées. Ces vulnérabilités incluent les questions de confidentialité, l'usurpation d'identité et la capture, les attaques de dictionnaire, les attaques de texte en clair connu, les attaques en répétition, les attaques de la négociation, la fausse identité, les attaques par interposition, la séparation de l'authentificateur et du serveur d'authentification, les bases de données multiples.

4.3.1 Questions de confidentialité

Comme les messages RADIUS peuvent contenir l'attribut User-Name ainsi que les attributs NAS-IP-Address ou NAS-Identifier, un attaquant qui espionne le trafic RADIUS peut être capable de déterminer la localisation géographique des homologues en temps réel. Dans les réseaux sans fil, il est souvent supposé que le trafic RADIUS est physiquement sûr, car il voyage normalement sur le réseau filaire et que cela limite la livraison des informations de localisation.

Cependant, il est possible à un attaquant authentifié d'usurper les paquets ARP [RFC826] afin de causer un détournement du trafic RADIUS sur le réseau sans fil. De cette façon, un attaquant peut obtenir des paquets RADIUS à partir desquels il peut glaner des informations de localisation de l'homologue, ou qu'il peut soumettre à une attaque de texte en clair connu ou de dictionnaire hors ligne. Pour traiter ces vulnérabilités, les mises en œuvre de la présente spécification DEVRAIENT utiliser IPsec ESP avec transformation non nulle et le chiffrement, l'authentification, la protection d'intégrité et contre la répétition par paquet pour protéger à la fois le trafic d'authentification [RFC2865] et de comptabilité [RFC2866] RADIUS, comme décrit au paragraphe 4.2.

4.3.2 Usurpation d'identité et capture

Les paquets Access-Request avec un attribut User-Password établissent l'identité de l'utilisateur et du NAS qui envoie le Access-Request, à cause de la façon dont le secret partagé entre le NAS et le serveur RADIUS est utilisée. Les paquets Access-Request avec des attributs CHAP-Password ou EAP-Message n'ont pas d'attribut User-Password. Par suite, l'attribut Message-Authenticator DEVRAIT être utilisé dans les paquets Access-Request qui n'ont pas d'attribut User-Password, afin d'établir l'identité du NAS qui envoie la requête.

Un attaquant peut tenter d'injecter des paquets dans la conversation entre le NAS et le serveur RADIUS, ou entre le serveur RADIUS et le serveur de sécurité. RADIUS [RFC2865] ne prend pas en charge le chiffrement autre que de cacher l'attribut. Comme décrit dans la [RFC2865], seuls les paquets Access-Reply et Access-Challenge sont protégés en intégrité. De plus, le mécanisme par paquet d'authentification et de protection de l'intégrité décrit dans la [RFC2865] a des faiblesses connues [MD5Attack], qui en font une cible tentante pour des attaquants qui cherchent à subvertir RADIUS/EAP.

Pour fournir une sécurité plus forte, l'attribut Message-Authenticator DOIT être utilisé dans tous les paquets RADIUS qui contiennent un attribut EAP-Message. Les mises en œuvre de la présente spécification DEVRAIENT utiliser IPsec ESP avec transformation non nulle et chiffrement, l'authentification, et la protection de l'intégrité et contre la répétition par paquet, comme décrit au paragraphe 4.2.

4.3.3 Attaques de dictionnaire

Le secret partagé RADIUS est vulnérable à l'attaque de dictionnaire hors ligne, fondée sur la capture de l'attribut Response-Authenticator ou Message-Authenticator. Afin de diminuer le niveau de vulnérabilité, la [RFC2865] recommande que le secret (mot de passe partagé entre le client et le serveur RADIUS) DEVRAIT être au moins aussi grand et non devinable qu'un mot de passe bien choisi. Il est préféré que le secret fasse au moins 16 octets. Le risque d'une attaque de dictionnaire hors ligne peut être encore réduit en employant IPsec ESP avec une transformation non nulle afin de chiffrer la conversation RADIUS, comme décrit au paragraphe 4.2.

4.3.4 Attaques de texte en clair connu

Comme EAP [RFC2284] ne prend pas en charge PAP, l'attribut RADIUS User-Password n'est pas utilisé pour porter les mots de passe d'utilisateur cachés dans les conversations RADIUS/EAP. Le mécanisme de dissimulation du mot de passe d'utilisateur, défini dans la [RFC2865] utilise MD5, défini dans la [RFC1321], afin de générer un flux de clés fondé sur le secret partagé RADIUS et l'authentificateur de demande *(Request Authenticator)*. Lorsque PAP est utilisé, il est possible de collecter les flux de clés correspondants à une certaine valeur d'authentificateur de demande, en capturant les conversations RADIUS qui correspondent à une tentative d'authentification PAP, en utilisant un mot de passe connu. Comme le mot de passe d'utilisateur est connu, le flux de clés correspondant à une certain authentificateur de demande peut être déterminé et mémorisé.

Comme le flux de clés peut avoir été déterminé précédemment à partir d'une attaque de texte en clair connu, si l'authentificateur de demande se répète, les attributs chiffrés en utilisant le mécanisme de dissimulation d'attribut RADIUS devrait être considéré comme compromis. En plus de l'attribut User-Password, qui n'est pas utilisé avec EAP, cela inclut des attributs comme Tunnel-Password ([RFC2868] paragraphe 3.5) et les attributs MS-MPPE-Send-Key et MS-MPPE-Recv-Key ([RFC2548] paragraphe 2.4) qui incluent un champ de sel au titre de l'algorithme de dissimulation.

Pour éviter cela, la [RFC2865], Section 3 conseille que comme il est prévu que le même secret PEUT être utilisé pour s'authentifier avec des serveurs dans des régions géographiques disparates, le champ Request Authenticator DEVRAIT exhiber une unicité mondiale et temporelle.

Lorsque l'authentificateur de demande est répété, le champ Sel défini au paragraphe 2.4 de la [RFC2548] ne fournit pas de protection contre la compromission. C'est parce que MD5 [RFC1321], est utilisé plutôt que HMAC-MD5 [RFC2104] pour générer le flux de clés, qui est calculé à partir du secret partagé (S) de 128 bits de RADIUS, du Request Authenticator (R) de 128 bits, et du champ Sel (A), en utilisant la formule b(1) = MD5(S + R + A). Comme le champ Sel est placé à la fin, si l'authentificateur de demande se répète sur un réseau où PAP est utilisé, alors le flux de clés salé pourrait être calculé à partir du flux de clés User-Password en continuant le calcul MD5 fondé sur le champ Sel (A), qui est envoyé en clair.

Même si EAP ne prend pas en charge l'authentification PAP, une vulnérabilité de la sécurité peut quand même exister lorsque le même secret partagé RADIUS est utilisé pour cacher le mot de passe d'utilisateur ainsi que les autres attributs. Cela peut arriver, par exemple, si le même mandataire RADIUS traite les demandes d'authentification pour EAP et PAP.

La menace peut être atténuée en protégeant RADIUS par IPsec ESP avec transformation non nulle, comme décrit au paragraphe 4.2. Lorsque les secrets partagés RADIUS sont configurés, le secret partagé RADIUS utilisé par un NAS qui prend en charge EAP NE DOIT PAS être réutilisé par un NAS qui utilise l'attribut User-Password, car une hygiène inappropriée de secret partagé pourrait conduire à la compromission des attributs cachés.

4.3.5 Attaques en répétition

Le protocole RADIUS fournit seulement une prise en charge limitée à la protection contre la répétition. Les demandes d'accès RADIUS incluent une durée de vie via les 128 bits de l'authentificateur de demande. Cependant, le Request Authenticator n'est pas un compteur de répétitions. Comme les serveurs RADIUS ne peuvent pas tenir une antémémoire des authentificateurs de demande précédents, l'authentificateur de demande ne fournit pas de protection contre la répétition.

La comptabilité RADIUS [RFC2866] ne prend pas en charge la protection contre la répétition au niveau du protocole. Du fait du besoin de la prise en charge de la reprise sur défaillance entre les serveurs de comptabilité RADIUS, la protection contre la répétition fondée sur le protocole n'est pas suffisante pour empêcher des enregistrements de comptabilité dupliqués. Cependant, une fois acceptés par le serveur de comptabilité, les enregistrements de comptabilité dupliqués peuvent être détectés par l'utilisation des attributs Acct-Session-Id ([RFC2866] paragraphe 5.5) et Event-Timestamp ([RFC2869] paragraphe 5.3).

À la différence de l'authentification RADIUS, la comptabilité RADIUS n'utilise pas l'authentificateur de demande comme un nom occasionnel. L'authentificateur de demande contient plutôt un hachage MD5 calculé sur les attributs Code, Identifiant, Longueur du paquet de demande de comptabilité, plus le secret partagé. L'authentificateur de réponse *(Response Authenticator)* contient aussi un hachage MD5 calculé sur les champs Code, Identifiant et Longueur, le champ authentificateur de demande du paquet Demande de comptabilité auquel on répond, les attributs de réponse et le secret partagé.

Comme l'authentificateur de réponse de comptabilité dépend en partie de l'authentificateur de demande de comptabilité, il n'est pas possible de répéter une réponse de comptabilité sauf si l'authentificateur de demande se répète. Bien qu'il soit possible d'utiliser des méthodes EAP telles que EAP TLS [RFC2716] qui inclut des vérifications de vivacité sur les deux côtés, tous les messages EAP ne vont pas inclure de durée de vie, de sorte que la protection fournie est incomplète.

Une forte protection contre la répétition pour l'authentification et la comptabilité RADIUS peut être fournie en activant la protection IPsec contre la répétition avec RADIUS, comme décrit au paragraphe 4.2.

4.3.6 Attaques sur la négociation

Dans une attaque sur la négociation, un NAS, serveur tunnel, mandataire RADIUS ou serveur RADIUS félon tente de causer le choix par l'homologue qui s'authentifie d'une méthode d'authentification moins sûre. Par exemple, une session qui

serait normalement authentifiée avec EAP va plutôt être authentifiée via CHAP ou PAP ; autrement, une connexion qui serait normalement authentifiée via une méthode EAP plus sûre telle que EAP-TLS [RFC2716] pourrait se trouver faite via une méthode EAP moins sûre, comme MD5-Challenge. La menace que font peser les appareils félons, qu'on pensait lointaine, a gagné en actualité grâce à la compromission des systèmes de commutation de compagnies de téléphone, comme celle décrite dans [Masters].

La protection contre les attaques sur la négociation exige l'élimination des négociations en dégradation. L'échange RADIUS peut être de plus protégé par l'utilisation de IPsec, comme décrit au paragraphe 4.2. Autrement, lorsque IPsec n'est pas utilisé, la vulnérabilité peut être atténuée via la mise en œuvre d'une politique par connexion de la part de l'homologue qui s'authentifie, et d'une politique par homologue de la part du serveur RADIUS. Pour l'homologue qui s'authentifie, la politique d'authentification devrait être établie sur la base de la connexion. Une politique par connexion permet à l'homologue qui s'authentifie de négocier une méthode EAP forte quand il se connecte à un service, tout en négociant une méthode EAP plus faible pour un autre service.

Avec une politique par connexion, un homologue qui s'authentifie va seulement tenter de négocier EAP pour une session dans laquelle la prise en charge de EAP est attendue. Par suite, il y a une présomption qu'un homologue qui s'authentifie en choisissant EAP exige ce niveau de sécurité. Si il ne peut pas être fourni, il est probable qu'il y a une mauvaise configuration de quelque sorte, ou même que l'homologue qui s'authentifie contacte le mauvais serveur. Si le NAS n'était pas capable de négocier EAP, ou si la EAP-Request envoyée par le NAS était d'un type EAP différent de celui qui est attendu, l'homologue qui s'authentifie DOIT se déconnecter. Un homologue qui s'authentifie en pensant que EAP va être négocié pour une session NE DOIT PAS négocier une méthode plus faible, comme CHAP ou PAP. Dans les réseaux sans fil, l'annonce de service elle-même peut être une mystification, de sorte qu'un attaquant pourrait tromper l'homologue et l'amener à négocier une méthode d'authentification convenable pour un réseau plus sûr.

Pour un NAS, il peut n'être pas possible de déterminer si un homologue est obligé de s'authentifier avec EAP jusqu'à ce que l'identité de l'homologue soit connue. Par exemple, pour les NAS à utilisation partagée, il est possible qu'un revendeur mette en œuvre EAP alors qu'un autre ne le fait pas. Autrement, certains homologues pourraient être authentifiés localement par le NAS tandis que d'autres homologues sont authentifiés via RADIUS. Dans ce cas, si des homologues du NAS DOIVENT faire EAP, le NAS DOIT alors tenter de négocier EAP pour toutes les sessions. Cela évite de forcer un homologue à prendre en charge plus d'un type d'authentification, ce qui pourrait affaiblir la sécurité.

Si CHAP est négocié, le NAS va passer les attributs User-Name et CHAP-Password au serveur RADIUS dans un paquet Access-Request. Si l'homologue n'est pas obligé d'utiliser EAP, le serveur RADIUS va alors répondre avec un paquet Access-Accept ou Access-Reject comme approprié. Cependant, si CHAP a été négocié mais qu'EAP est exigé, le serveur RADIUS DOIT répondre avec un paquet Access-Reject, plutôt que Access-Challenge/EAP-Message/Demande EAP. L'homologue qui s'authentifie DOIT refuser de renégocier l'authentification, même si la renégociation est de CHAP à EAP.

Si EAP est négocié mais n'est pas pris en charge par le mandataire ou serveur RADIUS, le serveur ou mandataire DOIT répondre avec un Access-Reject. Dans ces cas, un NAS PPP DOIT envoyer un LCP-Terminate et déconnecter l'homologue. C'est le comportement correct car l'homologue qui s'authentifie s'attend à ce que EAP soit négocié, et cette attente ne peut pas être satisfaite. Un homologue à capacité EAP qui s'authentifie DOIT refuser de renégocier le protocole d'authentification si EAP avait été initialement négocié. Noter que des problèmes avec un mandataire RADIUS non capable d'EAP pourrait se révéler difficiles à diagnostiquer, car un homologue qui se connecte à partir d'une localisation (avec un mandataire à capacité EAP) pourrait être capable de s'authentifier avec succès via EAP, alors que le même homologue se connectant à partir d'une autre localisation (et rencontrant un mandataire incapable de EAP) pourrait être systématiquement déconnecté.

4.3.7 Fausse identité

La Section 3 de la [RFC2865] déclare : Un serveur RADIUS DOIT utiliser l'adresse IP de source du paquet UDP RADIUS pour décider quel secret partagé utiliser, afin que les demandes RADIUS puissent être relayées par un mandataire.

Quand des demandes RADIUS sont transmises par un mandataire, les attributs NAS-IP-Address ou NAS-IPv6-Address peuvent ne pas correspondre à l'adresse de source. Comme l'attribut NAS-Identifier n'a pas besoin de contenir un FQDN, cet attribut peut aussi ne pas correspondre à l'adresse de source, même indirectement, qu'un mandataire soit présent ou non.

Par suite, la vérification d'authenticité effectuée par un serveur ou mandataire RADIUS ne vérifie pas que les attributs d'identification de NAS sont corrects. Cela rend possible à un NAS félon de falsifier les attributs NAS-IP-Address, NAS-IPv6-Address ou NAS-Identifier au sein d'une demande d'accès RADIUS afin de se faire passer pour un autre NAS. Il est aussi possible à un NAS félon de falsifier les attributs d'identification de session comme Called-Station-Id, Calling-Station-Id, et Originating-Line-Info.

Cela pourrait tromper le serveur RADIUS et l'amener ensuite à envoyer des messages Disconnect ou CoA-Request [RFC3576] contenant des attributs d'identification de session falsifiés à un NAS ciblé par un attaquant.

Pour traiter ces vulnérabilités, les mandataires RADIUS DEVRAIENT vérifier si les attributs d'identification de NAS (NAS-IP-Address, NAS-IPv6-Address, NAS-Identifier) correspondent à l'adresse de source des paquets générés par le NAS. Lorsque il n'y a pas de correspondance, un Access-Reject DEVRAIT être envoyé, et une erreur DEVRAIT être enregistrée.

Cependant, une telle vérification peut n'être pas toujours possible. Comme l'attribut NAS-Identifier n'a pas besoin de correspondre à un FQDN, il peut ne pas se résoudre en une adresse IP à confronter à l'adresse de source. Aussi, lorsque il existe un NAT entre le client et le mandataire RADIUS, la vérification des attributs NAS-IP-Address ou NAS-IPv6-Address peut n'être pas faisable.

Pour permettre la vérification du NAS et des paramètres d'identification de session, les méthodes EAP peuvent prendre en charge l'échange sécurisé de ces paramètres entre l'homologue et le serveur EAP. Les attributs d'identification de NAS incluent NAS-IP-Address, NAS-IPv6-Address et Called-Station-Id ; les attributs d'identification de session incluent User-Name et Calling-Station-Id. L'échange sécurisé de ces paramètres entre l'homologue et le serveur EAP permet au serveur RADIUS de vérifier si les attributs fournis par le NAS correspondent à ceux fournis par l'homologue ; de même, l'homologue peut vérifier les paramètres fournis par le NAS par rapport à ceux fournis par le serveur EAP. Cela permet la détection d'un NAS félon.

4.3.8 Attaques par interposition

RADIUS fournit seulement la sécurité bond par bond, même lorsque IPsec est utilisé. Par suite, un attaquant qui obtient le contrôle d'un mandataire RADIUS pourrait tenter de modifier les paquets EAP en transit. Pour se protéger contre cela, les méthodes EAP DEVRAIENT incorporer leurs propres mécanismes de protection d'intégrité et d'authentification par paquet.

4.3.9 Séparation de l'authentificateur et du serveur d'authentification

Comme noté dans la [RFC2716], il est possible à l'homologue et l'authentificateur EAP de s'authentifier mutuellement, et de déduire une clé de session maîtresse (MSK, *Master Session Key*) pour une suite de chiffrement utilisée pour protéger le trafic de données suivant. Cela ne pose pas de problème chez l'homologue, car l'homologue et le client EAP résident sur la même machine ; tout ce qui est nécessaire est que le module de client EAP déduise et passe une clé de session transitoire (TSK, *Transient Session Key*) au module de chiffrement.

La situation est plus complexe quand EAP est utilisé avec RADIUS, car l'authentificateur et le serveur d'authentification peuvent ne pas résider sur le même hôte.

Dans le cas où l'authentificateur et le serveur d'authentification résident sur des machines différentes, il y a plusieurs implications pour la sécurité. D'abord, l'authentification mutuelle va se produire entre l'homologue et le serveur d'authentification, et non entre l'homologue et l'authentificateur. Cela signifie qu'il n'est pas possible à l'homologue de valider l'identité du NAS ou serveur tunnel à qui il parle, en utilisant seulement EAP.

Comme décrit au paragraphe 4.2, quand RADIUS/EAP est utilisé pour encapsuler des paquets EAP, IPsec DEVRAIT être utilisé pour fournir l'authentification, l'intégrité, la protection contre la répétition et la confidentialité paquet par paquet. L'attribut Message-Authenticator est aussi exigé dans les demandes d'accès RADIUS qui contiennent un attribut EAP-Message envoyé du NAS ou serveur tunnel au serveur RADIUS. Comme l'attribut Message-Authenticator implique une vérification d'intégrité du message HMAC-MD5, il est possible au serveur RADIUS de vérifier l'intégrité de la demande d'accès ainsi que l'identité du NAS ou serveur tunnel, même lorsque IPsec n'est pas utilisé. De même, les paquets Access-Challenge contenant un attribut EAP-Message envoyé du serveur RADIUS au NAS sont aussi authentifiés et protégés en intégrité en utilisant une vérification d'intégrité de message HMAC-MD5, permettant au NAS ou serveur tunnel de déterminer l'intégrité du paquet et de vérifier l'identité du serveur RADIUS, même lorsque IPsec n'est pas utilisé. De plus, les paquets EAP envoyés en utilisant des méthodes qui contiennent leur propre protection d'intégrité ne peuvent pas être modifiés sans détection par un NAS ou serveur tunnel félon.

Le second problème qui se pose lorsque l'authentificateur et le serveur d'authentification résident sur des hôtes séparés est que la clé maîtresse de session (MSK, *Master Session Key*) EAP négociée entre l'homologue et le serveur d'authentification va devoir être transmise à l'authentificateur. Donc un mécanisme doit être fourni pour transmettre la MSK du serveur d'authentification au NAS ou serveur tunnel qui en a besoin. La spécification du mécanisme de transport de clé et

d'enveloppe sort du domaine d'application du présent document. Cependant, on s'attend à ce que le mécanisme d'enveloppe assure la confidentialité, la protection de l'intégrité et contre la répétition, et l'authentification de l'origine des données.

4.3.10 Bases de données multiples

Dans de nombreux cas, un serveur de sécurité va être déployé avec un serveur RADIUS afin de fournir des services EAP. Sauf si le serveur de sécurité fonctionne aussi comme serveur RADIUS, deux bases de données d'utilisateur séparées vont exister, chacune contenant des informations sur les exigences de sécurité pour l'utilisateur. Cela représente une faiblesse, car la sécurité peut être compromise par une attaque réussie contre l'un ou l'autre des serveurs, ou leurs bases de données. Avec plusieurs bases de données d'utilisateur, ajouter un nouvel utilisateur peut exiger plusieurs opérations, augmentant le risque d'erreurs. Les problèmes sont encore augmentés dans le cas où les informations d'utilisateur sont aussi conservées dans un serveur LDAP. Dans ce cas, trois mémorisations des informations d'utilisateur peuvent exister.

Afin de traiter ces menaces, la consolidation des bases de données est recommandée. Cela peut être réalisé en faisant que le serveur RADIUS et le serveur de sécurité mémorisent tous deux les information dans la même base de données, en faisant que le serveur de sécurité fournisse une pleine mise en œuvre RADIUS, ou en consolidant à la fois le serveur de sécurité et le serveur RADIUS sur la même machine.

5. Considérations relatives à l'IANA

La présente spécification ne crée aucun nouveau registre, ni ne définit aucun nouvel attribut ou valeur RADIUS.

6. Références

6.1 Références normatives

[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. *(MàJ par* RFC8174)

[RFC2279] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", janvier 1998. (*Obsolète, voir* RFC3629) *(D.S.)*

[RFC2284] L. Blunk, J. Vollbrecht, "Protocole extensible d'authentification (EAP) en PPP", mars 1998. (*Obs., voir* RFC3748) *(P.S.)*

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Ob., voir* RFC4303)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2486] B. Aboba, M. Beadles, "Identifiant d'accès réseau", janvier 1999. (*Obsolète, voir* RFC4282) *(P.S.)*

[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.)*

[RFC2988] V. Paxson, M. Allman, "Calcul du temporisateur de retransmission de TCP", novembre 2000. *(P.S.) (Obsolète, voir* RFC6298)

[RFC3162] B. Aboba, G. Zorn, D. Mitton, "RADIUS et IPv6", août 2001. *(P.S. ; MàJ par* RFC8044)

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC3576] M. Chiba et autres, "Extensions d'autorisation dynamique au service d'authentification distante d'utilisateur appelant (RADIUS)", juillet 2003. (*Obsolète, voir* RFC5176) *(Information)*

6.2 Références pour information

[IEEE802] ANSI/IEEE Std 802, "Standards for Local and Metropolitan Area Networks: Overview and Architecture", 1990.

[IEEE8021X] IEEE Std 802.1X-2001, "Standards for Local and Metropolitan Area Networks: Port based Network Access Control", juin 2001.

[Masters] Slatalla, M. and J. Quittner, "Masters of Deception." HarperCollins, New York, 1995.

[MD5Attack] Dobbertin, H., "The Status of MD5 After a Recent Attack", CryptoBytes Vol.2 No.2, Summer 1996.

[RFC0826] D. Plummer, "Protocole de résolution d'adresses Ethernet : conversion des adresses de protocole réseau en adresses Ethernet à 48 bits pour transmission sur un matériel Ethernet", STD 37, novembre 1982.

[RFC1510] J. Kohl et C. Neuman, "Service Kerberos d'authentification de réseau (v5)", septembre 1993. *(Obsolète, voir* RFC6649)

[RFC1661] W. Simpson, éditeur, "Protocole point à point (PPP)", STD 51, juillet 1994. *(MàJ par la* RFC2153)

[RFC2548] G. Zorn, "Attributs Microsoft spécifiques du fabricant pour RADIUS", mars 1999. *(Information)*

[RFC2607] B. Aboba, J. Vollbrecht, "Chaînage de mandataire et mise en œuvre de politique dans l'itinérance", juin 1999. *(Info.)*

[RFC2716] B. Aboba, D. Simon, "Protocole d'authentification des TLS d'EAP dans PPP" octobre 1999. (*Obs., voir* RFC5216) *(Exp.)*

[RFC2866] C. Rigney, "Comptabilité RADIUS", juin 2000. (*MàJ par* RFC2867, RFC5080) *(Information)*

[RFC2867] G. Zorn, B. Aboba, D. Mitton, "Modifications de la comptabilité RADIUS pour la prise en charge du protocole de tunnel", juin 2000. *(Information)*

[RFC2868] G. Zorn et autres, "Attributs RADIUS pour la prise en charge du protocole de tunnel", juin 2000. *(Information)*

[RFC2869] C. Rigney, W. Willats, P. Calhoun, "Extensions à RADIUS", juin 2000. (*MàJ par* RFC3579, RFC5080) *(Information)*

[RFC2983] D. Black, "Services différenciés et tunnels", octobre 2000. *(Information)*

[RFC3580] P. Congdon et autres, "Lignes directrices pour l'utilisation du service d'authentification distante d'utilisateur appelant (RADIUS) par IEEE 802.1X", septembre 2003. *(Information)*

[RFC4005] P. Calhoun et autres, "Application de serveur d'accès réseau Diameter", août 2005. *(P.S.) (Remplacée par* RFC7155)

Appendice A. Exemples

Les exemples ci-dessous illustrent des conversations entre un homologue qui s'authentifie, un NAS, et un serveur RADIUS. Les protocoles OTP et EAP-TLS sont utilisés seulement à des fins d'illustration ; d'autres protocoles d'authentification pourrait aussi être utilisés, bien qu'ils puissent présenter un comportement un peu différent.

Lorsque the NAS envoie une EAP-Request/Identity comme paquet initial, l'échange apparaît comme suit :

Homologue qui s'authentifie NAS Serveur RADIUS

```
                        <- EAP-Request/Identity
EAP-Response/Identity (MyID) ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/(MyID) ->
                                                <- RADIUS Access-Challenge/EAP-Message/EAP-Request
                                                  OTP/OTP Challenge
                        <- EAP-Request/OTP/OTP Challenge
EAP-Response/OTP, OTPpw ->
                        RADIUS Access-Request/
                        EAP-Message/EAP-Response/
                        OTP, OTPpw ->
                                                <- RADIUS Access-Accept/
                                                EAP-Message/EAP-Success (autres attributs)
                        <- EAP-Success
```

Dans le cas où le NAS s'initie avec une EAP-Request pour EAP TLS [RFC2716], et où l'identité est déterminée sur la base du contenu du certificat du client, l'échange va apparaître comme suit :

Homologue qui s'authentifie NAS Serveur RADIUS

```
                      <- EAP-Request/EAP-Type=EAP-TLS
                         (au début de TLS, le bit S est établi)
EAP-Response/EAP-Type=EAP-TLS
(TLS client_hello)->
                          RADIUS Access-Request/
                          EAP-Message/EAP-Response/
                          EAP-Type=EAP-TLS->
                                                <-RADIUS Access-Challenge/EAP-Message/
                                                EAP-Request/EAP-Type=EAP-TLS
                          <- EAP-Request/EAP-Type=EAP-TLS
                          (TLS server_hello, TLS certificate,
                          [TLS server_key_exchange,]
                          [TLS certificate_request,] TLS server_hello_done)
EAP-Response/EAP-Type=EAP-TLS
(TLS certificate, TLS client_key_exchange,
[TLS certificate_verify,]
TLS change_cipher_spec, TLS fini)->
                          RADIUS Access-Request/
                          EAP-Message/EAP-Response/
                          EAP-Type=EAP-TLS->
                                                <-RADIUS Access-Challenge/EAP-Message/
                                                EAP-Request/EAP-Type=EAP-TLS
                          <- EAP-Request/EAP-Type=EAP-TLS
                          (TLS change_cipher_spec, TLS fini)

EAP-Response/EAP-Type=EAP-TLS ->
                          RADIUS Access-Request/
                          EAP-Message/EAP-Response/
                          EAP-Type=EAP-TLS->
                                                <-RADIUS Access-Accept/EAP-Message/EAP-Success
                                                (autres attributs)
                          <- EAP-Success
```

Dans le cas où le NAS envoie d'abord un paquet EAP-Start au serveur RADIUS, la conversation apparaîtrait comme suit :

```
Homologue qui s'authentifie      NAS                    Serveur RADIUS
                          RADIUS Access-Request/EAP-Message/Start ->
                                                  <- RADIUS Access-Challenge/
                                                  EAP-Message/EAP-Request/Identity
                          <- EAP-Request/Identity
EAP-Response/Identity (MyID) ->
                          RADIUS Access-Request/
                          EAP-Message/EAP-Response/Identity (MyID) ->
                                                  <- RADIUS Access-Challenge/
                                                  EAP-Message/EAP-Request/OTP/OTP Challenge
                          <- EAP-Request/OTP/OTP Challenge
EAP-Response/OTP, OTPpw ->
                          RADIUS Access-Request/
                          EAP-Message/EAP-Response/OTP, OTPpw ->
                                                  <- RADIUS Access-Accept/
                                                  EAP-Message/EAP-Success (autres attributs)
                          <- EAP-Success
```

Dans le cas où le NAS s'initie avec une EAP-Request pour EAP TLS [RFC2716], mais où l'homologue répond avec un NAK, indiquant qu'il préférerait une autre méthode non mise en œuvre localement sur le NAS, l'échange va apparaître comme suit :

```
Homologue qui s'authentifie      NAS                    Serveur RADIUS
                          <- EAP-Request/EAP-Type=EAP-TLS
                          (au début de TLS, le bit S est établi)
EAP-Response/EAP-Type=NAK
(Alternative(s))->
                          RADIUS Access-Request/EAP-Message/
                          EAP-Response/NAK ->
                                                  <- RADIUS Access-Challenge/
                                                  EAP-Message/EAP-Request/Identity
                          <- EAP-Request/Identity
EAP-Response/Identity (MyID) ->
                          RADIUS Access-Request/
                          EAP-Message/EAP-Response/(MyID) ->
                                                  <- RADIUS Access-Challenge/
                                                  EAP-Message/EAP-Request OTP/OTP Challenge
                          <- EAP-Request/OTP/OTP Challenge
EAP-Response/OTP, OTPpw ->
                          RADIUS Access-Request/
                          EAP-Message/EAP-Response/OTP, OTPpw ->
                                                  <- RADIUS Access-Accept/
                                                  EAP-Message/EAP-Success (autres attributs)
                          <- EAP-Success
```

Dans le cas où l'homologue qui s'authentifie tente d'authentifier le NAS, la conversation apparaîtrait comme suit :

```
Homologue qui s'authentifie      NAS                    Serveur RADIUS
EAP-Request/Challenge, MD5 ->
                            RADIUS Access-Request/
                            EAP-Message/EAP-Request/Challenge, MD5 ->
                                                  <- RADIUS Access-Reject/EAP-Message/
                                                  EAP-Response/NAK (pas d'alternative)

                            <- EAP-Response/Nak (pas d'alternative)
EAP-Failure ->
```

Dans le cas où une réponse EAP invalide est insérée par un attaquant, la conversation apparaîtrait comme suit :

```
Homologue qui s'authentifie          NAS                    Serveur RADIUS
                              <- EAP-Request/EAP-Type=Foo
EAP-Response/EAP-Type=Foo ->
                              RADIUS Access-Request/
                              EAP-Message/EAP-Response/EAP-Type=Foo ->
                                                    <- RADIUS Access-Challenge/
                                                    EAP-Message/EAP-Request/EAP-Type=Foo
                              <- EAP-Request/EAP-Type=Foo
Faux de l'attaquant :
EAP-Response/EAP-Type=Bar ->

Légitime :
EAP-Response/EAP-Type=Foo ->
                              RADIUS Access-Request/
                              EAP-Message/EAP-Response/EAP-Type=Bar ->
                                                    <- RADIUS Access-Challenge/
                                                    EAP-Message/EAP-Request/EAP-Type=Foo,
                                                    Error-Cause="Paquet EAP invalide (Ignoré)"
                              RADIUS Access-Request/
                              EAP-Message/EAP-Response/EAP-Type=Foo ->
                                                    <- Access-Accept/EAP-Message/Success
                              <- EAP Success
```

Dans le cas où le client échoue à l'authentification EAP, et où un message d'erreur est envoyé avant la déconnexion, la conversation apparaîtrait comme suit :

```
Homologue qui s'authentifie          NAS                    Serveur RADIUS
                                RADIUS Access-Request/EAP-Message/Start ->
                                                    <- RADIUS Access-Challenge/
                                                    EAP-Message/EAP-Response/Identity
                              <- EAP-Request/Identity
EAP-Response/Identity (MyID) ->
                              RADIUS Access-Request/
                              EAP-Message/EAP-Response/(MyID) ->
                                                    <- RADIUS Access-Challenge/
                                                    EAP-Message/EAP-RequestOTP/OTP Challenge
                              <- EAP-Request/OTP/OTP Challenge
EAP-Response/OTP, OTPpw ->
                              RADIUS Access-Request/
                              EAP-Message/EAP-Response/OTP, OTPpw ->
                                                    <- RADIUS Access-Challenge/
                                                    EAP-Message/EAP-Request/Notification
                              <- EAP-Request/Notification
EAP-Response/Notification ->
                              RADIUS Access-Request/
                              EAP-Message/EAP-Response/Notification ->
                                                    <- RADIUS Access-Reject/
                                                    EAP-Message/EAP-Failure
                              <- EAP-Failure (client déconnecté)
```

Dans le cas où le serveur ou mandataire RADIUS ne prend pas en charge EAP-Message, mais où aucun message d'erreur n'est envoyé, la conversation apparaîtrait comme suit :

```
Homologue qui s'authentifie          NAS                    Serveur RADIUS
                               RADIUS Access-Request/
                               EAP-Message/Start ->
                                                    <- RADIUS Access-Reject
                               (Usager déconnecté)
```

Dans le cas où le serveur RADIUS local prend en charge EAP-Message, mais où le serveur RADIUS ne le fait pas, la

conversation apparaîtrait comme suit :

```
Homologue qui s'authentifie        NAS                    Serveur RADIUS
                              RADIUS Access-Request/EAP-Message/Start ->
                                                          <- RADIUS Access-Challenge/
                                                          EAP-Message/EAP-Response/Identity
                                 <- EAP-Request/Identity
EAP-Response/Identity(MyID) ->
                                 RADIUS Access-Request/
                                 EAP-Message/EAP-Response/(MyID) ->
                                                          <- RADIUS Access-Reject
                                                          (relayé par mandataire du serveur RADIUS distant)
                                 (Usager déconnecté)
```

Dans le cas où la liaison est PPP et où l'homologue qui s'authentifie ne prend pas en charge EAP, mais où EAP est exigé pour cet utilisateur, la conversation apparaîtrait comme suit :

```
Homologue qui s'authentifie        NAS                    Serveur RADIUS
                                 <- PPP LCP Request-EAP auth
PPP LCP NAK-EAP auth ->
                                 <- PPP LCP Request-CHAP auth
PPP LCP ACK-CHAP auth ->
                                 <- PPP CHAP Challenge
PPP CHAP Response ->
                                 RADIUS Access-Request/User-Name,
                                 CHAP-Password ->
                                                          <- RADIUS Access-Reject
                                 <-  PPP LCP Terminé
                                 (Usager déconnecté)
```

Dans le cas où la liaison est PPP, le NAS ne prend pas en charge EAP, mais EAP est exigé pour cet utilisateur, la conversation apparaîtrait comme suit :

```
Homologue qui s'authentifie        NAS                    Serveur RADIUS
                                 <- PPP LCP Request-CHAP auth
PP LCP ACK-CHAP auth ->
                                 <- PPP CHAP Challenge
PPP CHAP Response ->
                                 RADIUS Access-Request/User-Name,
                                 CHAP-Password ->
                                                          <- RADIUS Access-Reject
                                 <-  PPP LCP Terminé
                                 (Usager déconnecté)
```

Appendice B. Liste des changements

Les changements suivants ont été faits par rapport à la RFC 2869:

Un NAS peut simultanément prendre en charge l'authentification locale et le rôle d'intermédiaire ; une fois que le NAS entre en mode intermédiaire dans une session, il ne peut pas revenir à l'authentification locale. EAP est aussi explicitement décrit comme un protocole "verrouillé" (Section 2).

Le NAS peut s'initier avec une demande EAP pour un type d'authentification. Si la demande reçoit un NAK, le NAS devrait envoyer une demande d'accès initiale avec un attribut EAP-Message contenant un EAP-Response/NAK.

Le serveur RADIUS peut traiter une réponse EAP invalide comme une erreur non fatale (paragraphe 2.2).

Pour l'utilisation avec RADIUS/EAP, les attributs Password-Retry (paragraphe 2.3) et Reply-Message (2.6.5) sont déconseillés.

Chaque session EAP a un espace d'identifiant univoque (paragraphe 2.6.1).

L'inversion de rôle n'est pas prise en charge (paragraphe 2.6.2).

Les combinaisons de messages (par exemple Access-Accept/EAP-Failure) qui sont en conflit sont déconseillées (paragraphe 2.6.3).

Un seul paquet EAP peut être encapsulé dans un message RADIUS (paragraphe 3.1).

Une demande d'accès sans authentification explicite ni attribut Message-Authenticator DEVRAIT être éliminée en silence (paragraphe 3.3).

L'attribut Originating-Line-Info est pris en charge (paragraphe 3.3).

IPsec ESP avec transformation non-nulle DEVRAIT être utilisé et le modèle d'usage est décrit en détails (paragraphe 4.2).

Une discussion supplémentaires des vulnérabilités (paragraphe 4.1) et des correctifs potentiels (paragraphe 4.3).

Séparation des références normatives (paragraphe 6.1) et pour information (paragraphe 6.2).

Ajout d'exemples supplémentaires (Appendice A) : un NAS s'initiant avec une demande EAP pour un type d'authentification ; tentative d'inversion de rôle.

Déclaration de propriété intellectuelle

Remerciements

Merci à Dave Dawson et Karl Fox de Ascend, Glen Zorn de Cisco Systems, Jari Arkko de Ericsson et Ashwin Palekar, Tim Moore et Narendra Gidwani de Microsoft pour les utiles discussions de cet espace de problème. Les auteurs tiennent aussi à remercier Tony Jeffree, président de IEEE 802.1 pour son assistance à résoudre les problèmes de RADIUS/EAP dans IEEE 802.1X-2001.

Adresse des auteurs

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA
téléphone : +1 425 706 6605
Fax: +1 425 936 7329

Pat R. Calhoun
Airespace
110 Nortech Parkway
San Jose, California, 95134
USA
téléphone : +1 408 635 2023
Fax: +1 408 635 2020

mél : bernarda@microsoft.com

mél : pcalhoun@airespace.com

Déclaration complète de droits de reproduction

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