Groupe de travail Réseau
Request for Comments : 5124
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. Ott, Helsinki University of Technology
E. Carrara, KTH

février 2008

Profil RTP sécurisé étendu pour rétroaction fondée sur le protocole de contrôle de transport en temps réel (RTCP)

Résumé
Un profil RTP (SAVP) pour les communications sûres en temps réel et un autre profil (AVPF) pour fournir des rétroactions en temps utile de la part des receveurs à un envoyeur sont définis respectivement dans les RFC 3711 et RFC 4585. Le présent mémoire spécifie la combinaison des deux profils pour permettre des communications RTP sûres avec rétroaction.

Table des Matières

1. Introduction

Le protocole de transport en temps réel, le protocole de contrôle de RTP associé (RTP/RTCP) [RFC3550], et le profil pour les communications audiovisuelles avec contrôle minimal [RFC3551] définissent des mécanismes pour transmettre des supports en temps réel à travers un réseau IP. RTP donne les moyens de préserver le rythme et détecter la perte de paquet, entre autres choses, et les formats de charge utile RTP assurent un tramage approprié des supports (en continu) dans un environnement fondé sur le paquet. RTCP permet aux receveurs de fournir des rétroactions sur la qualité de réception et permet à tous les membres d'une session RTP d'en savoir plus sur chaque autre.

La spécification RTP fournit seulement une prise en charge rudimentaire du chiffrement de RTP et des paquets RTCP. RTP sécurisé [RFC3711] définit un profil RTP ("SAVP") pour des sessions de supports RTP sécurisées, définissant des méthodes pour un chiffrement approprié des paquets RTP et RTCP, la protection de l'intégrité et contre la répétition. La négociation initiale de SRTP et de ses paramètres de sécurité doit être faite hors bande, par exemple, en utilisant le

protocole de description de session (SDP, *Session Description Protocol*) [RFC4566] avec les extensions pour porter le matériel de chiffrement [RFC4567], [RFC4568].

La spécification RTP donne aussi un soutien limité à des rétroactions en temps utile des receveurs aux envoyeurs, normalement au moyen de statistiques de réception rapportant à des intervalles assez réguliers selon la taille du groupe, la taille moyenne de paquet RTCP, et la bande passante RTCP disponible. Le profil étendu de RTP avec rétroactions fondées sur RTCP ("AVPF") [RFC4585] permet aux participants à la session de fournir statistiquement des rétroactions immédiates tout en maintenant le débit moyen de données RTCP pour tous les envoyeurs. Comme pour SAVP, l'utilisation de AVPF et de ses paramètres doit être négociée hors bande au moyen de SDP [RFC4566] et des extensions définies dans la [RFC4585].

SRTP et AVPF sont tous deux des profils RTP et doivent être négociés. Cela implique que l'un et/ou l'autre peut être utilisé, mais les deux profils ne peuvent pas être négociés pour la même session RTP (en utilisant une description SDP de niveau session). Cependant, l'utilisation conjointe de communications sécurisées et de rétroactions en temps utile est désirable. Donc, le présent document spécifie un nouveau profil RTP ("SAVPF") qui combine les caractéristiques de SAVP et AVPF.

Comme SAVP et AVPF sont largement orthogonaux, la combinaison des deux est presque directe. Aucun algorithme sophistiqué n'a besoin d'être spécifié dans ce document. À la place, on fait référence aux deux profils existants et seules les implications de leur combinaison et les variantes possible à partir des règles des profils existants sont décrites dans le processus de négociation.

1.1 Définitions

Les définitions des [RFC3550], [RFC3551], [RFC4585], et [RFC3711] s'appliquent.

Les définitions suivantes sont spécifiquement utilisées dans le présent document:

Session RTP : association entre un ensemble de participants communiquant avec RTP comme défini dans la [RFC3550].

Description de supports (SDP) : ce terme se réfère à la spécification donnée dans une seule m= line dans un message SDP. Une description de supports SDP peut définir seulement une session RTP.

Session de supports : ce terme se réfère à une collection de descriptions de supports SDP qui sont sémantiquement groupées pour représenter des solutions de remplacement des mêmes moyens de communications. Hors d'un tel groupe, il va en être négocié ou choisi un pour une relation de communication et la session RTP correspondante va être instanciée. Si aucun paramètre de session commun convenable pour les points d'extrémité impliqués ne peut être trouvé, la session de supports va être rejetée. Dans le cas le plus simple, une session de supports est équivalente à une description de supports SDP et équivalente à une session RTP.

1.2 Terminologie

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 le BCP 14, [RFC2119].

2. Règles de SAVPF

SAVP est défini comme une couche intermédiaire entre RTP (suivant le profil RTP AVP régulier) et la couche de transport (généralement UDP). Cela donne une hiérarchie à deux couches au sein du protocole de transport en remps réel. Dans SAVPF, la couche supérieure (AVP) est remplacée par le profil RTP étendu par des rétroactions (AVPF).

AVPF modifie les règles de rythme pour la transmission des paquets RTCP et ajoute des formats de paquet RTCP supplémentaires spécifiques de la rétooaction. Ces fonctions sont indépendantes du chiffrement et/ou de la protection de l'intégrité ultérieurs des paquets RTCP. Le fonctionnement de la couche AVPF reste inchangé dans SAVPF.

Le profil AVPF déduit de la [RFC3550] l'utilisation (facultative) du préfixe de chiffrement pour RTCP. Le préfixe de chiffrement NE DOIT PAS être utilisé dans le profil SAVPF (il n'est pas utilisé dans SAVP, car il est seulement applicable à la méthode de chiffrement spécifiée dans la [RFC3550]).

La partie SAVP utilise des champs supplémentaires ajoutés à la fin des paquets RTP et RTCP et exécute des transformations cryptographiques sur le contenu (de certains) des paquets RTP/RTCP. Ce comportement reste inchangé dans SAVPF. Le calcul de la taille moyenne de paquet RTCP fait par la couche AVPF pour les besoins du rythme DOIT tenir compte des champs ajoutés par la couche SAVP.

La partie SRTP ne devient active que quand le RTP ou RTCP a été programmé par la couche AVPF "supérieure" ou reçu du protocole de transport, sans considération de son rythme et contenu.

2.1 Formats de paquet

AVPF définit des formats de paquet supplémentaires pour fournir des informations de rétroaction. Ces formats de paquet supplémentaires définis dans la [RFC4585] (et d'autres définis ailleurs pour être utilisés avec AVPF) PEUVENT être utilisés avec SAVPF.

SAVP définit un format de paquet modifié pour les paquets SRTP et SRTCP qui consiste essentiellement en les formats de paquet RTP/RTCP plus des champs de queue pour des besoins de sécurité. Pour SAVPF, tous les paquets RTCP DOIVENT être encapsulés comme défini au paragraphe 3.4 de la [RFC3711].

2.2 Extensions

Les extensions aux paquets de rétroaction AVPF RTCP définis ailleurs PEUVENT être utilisés avec le profil SAVPF pourvu que ces extensions soient en conformité avec les règles d'extension de la [RFC4585].

Des extensions supplémentaires (par exemple, des transformations) définies pour SAVP suivant les règles de la Section 6 de la [RFC3711] PEUVENT aussi être utilisées avec le profil SAVPF. Les frais généraux par paquet RTCP dépendent des extensions et transformations choisies. De nouvelles extensions et transformations ajoutées à l'avenir PEUVENT introduire d'autres frais généraux par paquet encore inconnus.

Finalement, d'autres extensions spécifiques de SAVPF PEUVENT être définies ailleurs.

2.3 Implications de la combinaison de AVPF et de SAVP

Le profil AVPF vise -- statistiquement -- à permettre aux receveurs de fournir des rétroactions en temps utile aux envoyeurs. La fréquence à laquelle il est permis en moyenne aux receveurs d'envoyer des informations de rétroaction dépend de la bande passante de RTCP, de la taille du groupe, et de la taille moyenne d'un paquet RTCP. SRTCP (voir le paragraphe 3.4 de la [RFC3711]) ajoute des champs supplémentaires (dont certains sont de longueur configurable) à la fin de chaque paquet RTCP qui sont probablement d'au moins 10 à 20 octets (14 octets par défaut). Noter que les extensions et transformations définies à l'avenir, ainsi que la configuration de chaque longueur de champ, PEUT ajouter des frais généraux supérieurs. En utilisant SRTP, la taille moyenne d'un paquet RTCP va augmenter et donc réduire la fréquence permise de fourniture des rétroactions (en temps utile). Les concepteurs d'application doivent avoir conscience de cela, et prendre des précautions pour que les parts de bande passante RTCP soient maintenues. Cela DOIT être fait en ajustant la variable RTCP "avg_rtcp_size" pour qu'elle reflète la taille des paquets SRTCP.

3. Définitions SDP

3.1 Définition du profil

Les profils d'AV définis dans les [RFC3551], [RFC4585], et [RFC3711] sont appelés respectivement "AVP", "AVPF", et "SAVP", dans le contexte, par exemple, du protocole de description de session (SDP) [RFC4585]. Le profil combiné spécifié dans le présent document est appelé "SAVPF".

3.2 Définitions d'attributs

Les attributs SDP pour négocier les sessions SAVP sont définis dans la [RFC4567] et la [RFC4568]. Ces attributs PEUVENT aussi être utilisés avec SAVPF. Les règles définies dans les [RFC4567] et [RFC4568] s'appliquent.

Les attributs SDP pour négocier les sessions AVPF sont définies dans la [RFC4585]. Ces attributs PEUVENT aussi être utilisés avec SAVPF. Les règles définies dans la [RFC4585] s'appliquent.

3.3 Négociation de profil

Les descriptions de sessions RTP peuvent être convoyées en utilisant des protocoles dédiés aux communications multimédia comme du modèle SDP d'offre/réponse ([RFC3264]) utilisé avec le protocole d'initialisation de session (SIP) [RFC3261], le protocole de flux en temps rée (RTSP, *Real Time Streaming Protocol*) [RFC2326], ou le protocole d'annonce de session (SAP, *Session Announcement Protocol*) [RFC2974], mais peuvent aussi être distribués en utilisant la messagerie électronique, NetNews, des pages de la Toile, etc.

Le modèle d'offre/répose permet que les paramètres de session résultants soient négociés en utilisant les attributs SDP définis dans les [RFC4567] et [RFC4568]. Dans les paragraphes qui suivent, le processus de négociation est décrit dans les termes du modèle d'offre/réponse.

Ensuite, les cas qui n'utilisent pas le modèle d'offre/réponse sont traités : la prise en charge de la négociation spécifique de RTSP est fournie par la [RFC4567] comme exposé au paragraphe 3.3.2, et la prise en charge des annonces SAP (sans négociation du tout) est traitée au paragraphe 3.3.3.

3.3.1 Négociation fondée sur l'offre/demande des descriptions de session

Les négociations (par exemple, de profils RTP, codecs, adresses de transport, etc.) sont effectuées sur la base de la session de supports (par exemple, par m= line dans SDP). Si la négociation d'une session de supports échoue, d'autres PEUVENT quand même réussir.

Différents profils RTP PEUVENT être utilisés dans différentes sessions de supports. Pour négocier une description de supports, les quatre profils AVP, AVPF, SAVP, et SAVPF sont mutuellement exclusifs. Noter cependant que des entités SAVP et SAVPF PEUVENT être mélées dans une seule session RTP (voir la Section 4). Aussi, le mécanisme d'offre/réponse PEUT être utilisé pour offrir des solutions de remplacement pour la même session de supports et permettre à celui qui répond de choisir un des profils.

Pourvu qu'un mécanisme offrant des profils de sécurité de remplacement devienne disponible (comme l'est présentement en développement dans la [RFC5939]) un offreur capable de prendre en charge plus d'un de ces profils pour une certaine session de supports DEVRAIT toujours offrir toutes les solutions de remplacement acceptables dans une certaine situation. Les solutions de remplacement DEVRAIENT être offertes dans l'ordre de préférence et l'offreur DEVRAIT préférer les profils sûr à ceux qui ne le sont pas. L'offre NE DEVRAIT PAS inclure à la fois une solution de remplacement sûre (SAVP et SAVPF) et une non sûre (par exemple, AVP et AVPF) dans la même offre car cela peut permettre des attaques en dégradation et autres. Donc, si des profils RTP sûrs et non sûrs sont offerts à la fois (par exemple, pour un SRTP au mieux [RFC5939]) la signalisation de négociation DOIT être protégée de façon appropriée pour éviter de telles attaques.

Si une offre contient plusieurs profils, celui qui répond DEVRAIT préférer un profil sûr (si il le prend en charge) à un non sûr. Parmi les profils sûrs ou non sûrs, celui qui répond DEVRAIT choisir le premier acceptable pour respecter la préférence de l'offreur.

Si une description de supports dans une offre utilise SAVPF et si celui qui répond ne prend pas en charge SAVPF, la session de supports DOIT être rejetée.

Si une description de supports dans une offre ne prend pas en charge SAVPF mais si celui qui répond veut utiliser SAVPF, il DOIT rejeter la session de supports. Celui qui répond PEUT fournir une contre offre avec une description de supports indiquant SAVPF dans un échange d'offre/réponse initié ensuite.

3.3.2 Négociation fondée sur RTSP des descriptions de session

RTSP [RFC2326] ne prend pas en charge le modèle d'offre/réponse. Cependant, RTSP prend en charge l'échange de paramètres de session de supports (incluant des informations de profil et d'adresse) au moyen de l'en-tête Transport. La gestion de clés fondée sur SDP comme définie dans la [RFC4567] ajoute un en-tête RTSP (KeyMgmt) pour prendre en charge le transport d'un protocole de gestion de clés (incluant le matériel de chiffrement).

L'en-tête RTSP Transport PEUT être utilisé pour déterminer le profil pour la session de supports. Conceptuellement, les règles définies au paragraphe 3.3.1 s'appliquent en conséquence. Le fonctionnement détaillé est le suivant : une description SDP (par exemple, restituée du serveur RTSP au moyen de DESCRIBE) contient la description du flux de supports de la ressource RTSP particulière.

Le client RTSP DOIT choisir exactement un des profils par flux de supports qu'il veut recevoir. Il DOIT faire cela dans la demande SETUP. Le client RTSP DOIT indiquer le profil RTP choisi en indiquant le profil et l'adresse de transport

complète du serveur (adresse IP et numéro d'accès) dans l'en-tête Transport inclus dans la demande SETUP. La réponse du serveur RTSP au message SETUP du client DOIT confirmer son choix de profil ou refuser la demande SETUP (ce qu'il ne devrait pas faire après avoir offert d'abord les profils).

Note : pour changer un des profils utilisés, le client doit supprimer son flux de supports (et éventuellement toute la session RTSP) en utilisant la méhode TEARDOWN et la rétablir en utilisant SETUP. Cela peut changer aussitôt que la mise à jour des supports (similaire à un SIP UPDATE ou re-INVITE) est spécifiée.

Quand on utilise la gestion de clés SDP [RFC4567], l'en-tête KeyMgmt DOIT être inclus dans les messages RTSP appropriés si un profil sûr est choisi. Si différents profils sûrs sont offerts dans la description SDP (par exemple, SAVP et SAVPF) et si du matériel de chiffrement différent est fourni pour eux, après avoir choisi un profil dans le message SETUP, seul l'en-tête KeyMgmt pour celui choisi DOIT être fourni. Les règles pour la confrontation des en-têtes KeyMgmt aux flux de supports s'appliquent selon la [RFC4567].

3.3.3 Annonce des descriptions de session

Les protocoles qui ne permettent pas la négociation interactive des descriptions de session (par exemple, SAP [RFC2974], descriptions postées sur une page de la Toile ou envoyées par messagerie) portent la responsabilité de l'accès adéquat aux sessions de supports chez l'initiateur d'une session.

L'initiateur DEVRAIT fournir des descriptions de session de remplacement pour les multiples profils RTP pour autant qu'ils sont acceptables à l'application et à l'objet de la session. Si la sécurité est désirée, SAVP peut être offert comme solution de remplacement à SAVPF -- mais les sessions AVP ou AVPF NE DEVRAIENT PAS être annoncées si d'autres moyens de sécurité ne s'appuyant pas sur SRTP ne sont pas employés.

Les attributs SDP définis dans la [RFC4567] et la [RFC4568] peuvent aussi être utilisés pour la distribution du paramètre de sécurité des descriptions de session annoncées.

La description du schéma de sécurité défini dans la [RFC4568] exige qu'un canal de communications sûr empêche des tiers d'espionner et manipuler les paramètres de chifrement. Donc, la sécurité de SAP (comme définie dans la [RFC2974]), S/MIME [RFC3851], HTTPS [RFC2818], ou d'autres mécanismes convenables DEVRAIENT être utilisés pour distribuer ou accéder à ces descriptions de session.

3.3.4 Description de profils de session de remplacement

Les entités SAVP et SAVPF PEUT être mélangées dans la même session RTP (voir aussi la Section 4) et aussi le PEUVENT des entités AVP et AVPF. Les autres combinaisons -- c'est-à-dire, entre profils sûrs et non sûrs -- dans la même session RTP sont incompatibles et NE DOIVENT PAS être utilisées ensemble.

Si la négociation entre les homologues impliqués est possible (comme avec le modèle offre/réponse du paragraphe 3.3.1 ou RTSP au paragraphe 3.3.2) des profils de remplacement (sûrs et non sûrs) PEUVENT être spécifiés par une entité (par exemple, l'offreur) et un choix d'un profil DOIT être fait par l'autre. Si une telle négociation n'est pas possible (par exemple, avec SAP comme au paragraphe 3.3.3) des profils incompatibles NE DOIVENT PAS être spécifiés comme solutions de remplacement.

La négociation de profils de remplacement fera l'objet d'études ultérieures.

Des profils RTP PEUT être mélangés arbitrairement entre différentes sessions RTP.

3.4 Exemples

Ce paragraphe inclut des exemples d'utilisation de SDP pour négocier des profils sûrs et non sûrs. Selon le mécanisme de chiffrement utilisé et ses paramètres, les messages SDP exigent normalement la protection de l'intégrité et, pour certains mécanismes, vont aussi avoir besoin de la protection de la confidentialité. Par exemple, on pourrait dire que la protection de l'intégrité est exigée pour l'empreinte digitale a=fingerprint du protocole de sécurité de couche transport de datagramme - transport sécurisé en temps réel (DTLS-SRTP, *Datagram Transport Layer Security - Secure Real-time Transport Protocol*) [RFC5764], et la confidentialité est requise pour le a=crypto des descriptions de sécurité de la [RFC4568].

Exemple 1 : La description de session suivante indique une session sûre constituée d'audio et de multi fréquences bi-tonalités (DTMF, *dual tone multi-frequency*) pour une communication en point à point dans laquelle le flux DTMF utilise des NACK génériques. Le protocole de gestion de clés indiqué est MIKEY. Cette description de session (l'offre)

pourrait être contenue dans un message SIP INVITE ou 200 OK pour indiquer que son envoyeur est capable, et accepte, de recevoir des rétroactions pour le flux DTMF qu'il transmet. La réponse correspondante peut être portée dans un 200 OK ou un ACK. Les paramètres pour le protocole de sécurité sont négociés comme décrit par les extensions à SDP définies dans la [RFC4567].

```
v=0
o=alice 3203093520 3203093520 IN IP4 host.exemple.com
s=Supports avec rétroaction
t=0 0
c=IN IP4 host.exemple.com
m=audio 49170 RTP/SAVPF 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-16
a=rtcp-fb:96 nack
a=key-mgmt:mikey uiSDF9sdhs727ghsd/dhsoKkdOokdo7eWsnDSJD...
```

Exemple 2 : Cet exemple montre les mêmes paramètres de rétroaction que dans l'exemple 1 mais utilise la syntaxe des descriptions sécurisées [RFC4568]. Noter que la partie clé de l'attribut a=crypto n'est pas protégée contre l'espionnage et donc la description de session a besoin d'être échangée sur un canal de communication sûr.

```
v=0
o=alice 3203093520 3203093520 IN IP4 host.exemple.com
s=Supports avec rétroaction
t=0 0
c=IN IP4 host.exemple.com
m=audio 49170 RTP/SAVPF 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-16
a=rtcp-fb:96 nack
a=crypto:AES_CM_128_HMAC_SHA1_32
inline:d/16/14/NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj/2^20/1:32
```

Exemple 3 : Cet exemple est repris de l'exemple 1, mais montre l'interaction entre l'offreur et celui qui répond dans un échange d'offre/réponse, là encore en utilisant MIKEY pour négocier le matériel de chiffrement :

Offre :

```
v=0
o=alice 3203093520 3203093520 IN IP4 host.exemple.com
s=Supports avec rétroaction
t=0 0
c=IN IP4 host.exemple.com
a=key-mgmt:mikey uiSDF9sdhs727ghsd/dhsoKkdOokdo7eWsnDSJD...
m=audio 49170 RTP/SAVPF 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-16
a=rtcp-fb:96 nack
```

Réponse :

```
v=0
o=alice 3203093521 3203093521 IN IP4 host.another.exemple.com
s=Supports avec rétroaction
t=0 0
c=IN IP4 host.another.exemple.com
a=key-mgmt:mikey ushdgfdhgfuiweyfhjsgdkj2837do7eWsnDSJD...
m=audio 53012 RTP/SAVPF 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
```

```
a=fmtp:96 0-16
a=rtcp-fb:96 nack
```

Exemple 4 : Cet exemple montre l'échange de flux vidéo contrôlé via RTSP. Un client acquiert une description de supports d'un serveur en utilisant DESCRIBE et obtient une description SDP statique sans aucun paramètre de chiffrement, mais la description des supports montre que les deux sessions de supports sûres et non sûres utilisant (S)AVPF sont disponibles. Un mécanisme qui permet l'identification explicite de ces solutions de remplacement (c'est-à-dire, des sessions sûres et non sûres) dans la description de session est présentement défini [RFC5939]. Le client produit alors une demande SETUP et indique son choix en incluant le profil concerné dans le paramètre Transport. De plus, le client inclut un en-tête KeyMgmt pour porter ses paramètres de sécurité, qui est confronté à un en-tête KeyMgmt correspondant provenant du serveur dans la réponse. Une seule session de supports est choisie afin que l'URI RTSP agrégé soit suffisant pour l'identification.

Paire de demande-réponse RTSP DESCRIBE (facultative) :

```
DESCRIBE rtsp://movies.exemple.org/exemple RTSP/2.0
CSeq: 314
Accept: application/sdp

200 OK
CSeq: 314
Date: 25 Nov 2005 22:09:35 GMT
Content-Type: application/sdp
Content-Length: 316

v=0
o=alice 3203093520 3203093520 IN IP4 movies.exemple.com
s=Supports avec rétroaction
t=0 0
c=IN IP4 0.0.0.0
+-Solution un-------------------------+
|m=video 49170 RTP/SAVPF 96    |
|a=rtpmap:96 H263-2000/90000     |
|a=rtcp-fb:96 nack                        |
+-----------------------------------------+
+-Solution deux----------------------+
|m=video 49172 RTP/AVPF 96     |
|a=rtpmap:96 H263-2000/90000(  |
|a=rtcp-fb:96 nack                       |
+--------------------------------------+
```

Paire de demande-réponse RTSP SETUP :

```
SETUP rtsp://movies.exemple.org/exemple RTSP/2.0
CSeq: 315
Transport: RTP/SAVPF;unicast;dest_addr=":53012"/":53013"
KeyMgmt: prot=mikey;url="rtsp://movies.exemple.org/exemple";
         data="uiSDF9sdhs727ghsd/dhsoKkdOokdo7eWsnD..."

200 OK
CSeq: 315
Date: 25 Nov 2005 22:09:36 GMT
Session: 4711

Transport: RTP/SAVPF;unicast;dest_addr=":53012"/":53013";
         src_addr="192.0.2.15:60000"/"192.0.2.15:60001"
KeyMgmt: prot=mikey;url="rtsp://movies.exemple.org/exemple";
         data="ushdgfdhgfuiweyfhjsgdkj2837do7eWsnDSJD..."
Accept-Ranges: NPT, SMPTE
```

Exemple 5 : La description de session suivante indique une session audio/vidéo en diffusion groupée (utilisant le MIC loi µ pour l'audio et H.261 ou H.263+) avec la source vidéo qui accepte les NACK génériques pour les codecs et le choix

d'image de référence pour H.263. Les paramètres pour le protocole de sécurité sont négociés comme décrit par les extensions SDP définies dans la [RFC4567], utilisées au niveau session. Une telle description peut avoir été portée en utilisant le protocole d'annonce de session (SAP).

```
v=0
o=alice 3203093520 3203093520 IN IP4 host.exemple.com
s=Vidéo en diffusion groupée avec rétroactions
t=3203130148 3203137348
a=key-mgmt:mikey uiSDF9sdhs7494ghsd/dhsoKkdOokdo7eWsnDSJD...
m=audio 49170 RTP/SAVP 0
c=IN IP4 224.2.1.183
a=rtpmap:0 PCMU/8000
m=video 51372 RTP/SAVPF 98 99
c=IN IP4 224.2.1.184
a=rtpmap:98 H263-1998/90000
a=rtpmap:99 H261/90000
a=rtcp-fb:* nack
a=rtcp-fb:98 nack rpsi
```

4. Interfonctionnement des entités AVP, SAVP, AVPF, et SAVPF

Le profil SAVPF défini dans le présent document est une combinaison du profil SAVP [RFC3711] et du profil AVPF [RFC4585] (qui à son tour est une extension du profil RTP définie dans la [RFC3551]).

SAVP et SAVPF utilisent SRTP [RFC3711] pour réaliser la sécurité. AVP et AVPF utilisent RTP tout simple [RFC3550] et donc ne fournissent pas de sécurité (sauf si des mécanismes externes de sécurité sont appliqués comme expliqué au paragraphe 9.1 de la [RFC3550]). SRTP et RTP ne sont pas destinés à interopérer ; les entités respectives de protocole ne sont pas supposées faire partie de la même session RTP. Donc, AVP et AVPF d'un côté et SAVP et SAVPF de l'autre, NE DOIVENT PAS être mélangés.

Les entités RTP qui utilisent SAVP et les profils SAVPF PEUVENT être mélangées dans une seule session RTP. Les considérations d'interfonctionnement définies à la Section 5 de la [RFC4585] s'appliquent.

5. Considérations sur la sécurité

Le profil SAVPF hérite ses propriétés de sécurité du profil SAVP ; donc, il est soumis aux considérations sur la sécurité discutées dans la [RFC3711]. Comparé à SAVP, le profil SAVPF n'ajoute ni n'enlève aucun service de sécurité.

Il y a un désir de prise en charge de la sécurité des flux de supports et, en même temps, de rétro compatibilité avec les nœuds non SAVP(F).

Les concepteurs d'applications devraient avoir conscience que la sécurité NE DEVRAIT PAS être mise en balance avec l'interopérabilité. Si des informations sont à distribuer à des groupes fermés (c'est-à-dire, à la confidentialité protégée) il est RECOMMANDÉ de ne pas offrir d'autres solutions de remplacement que SAVP et SAVPF pour les sessions de support comme décrit aux paragraphes 3.3 et 3.4, sauf si d'autres mécanismes de sécurité vont être utilisés, par exemple, ceux décrits au paragraphe 9.1 de la [RFC3550]. De même, si la protection de l'intégrité est considérée comme importante, il est RECOMMANDÉ de ne pas offrir d'autres solution de remplacement que SAVP et SAVPF, sauf si d'autres mécanismes qui peuvent la garantir sont connus pour être en place, par exemple, des mécanismes de couche inférieure comme décrit à la Section 9 de la [RFC3550].

Offrir simultanément des profils sûrs et non sûrs peut ouvrir la porte à des attaques en dégradation. Donc, un tel mélange de profils offerts NE DEVRAIT PAS être fait.

Noter que les règles de partage des clés maîtresses s'appliquent comme décrit dans la [RFC3711] (par exemple, au paragraphe 9.1). En particulier, les mêmes règles pour éviter la répétition du bourrage (réutilisation de flux de clés) s'appliquent : une clé maîtressse NE DOIT PAS être partagée entre différentes sessions RTP sauf si les SSRC utilisées sont uniques à travers tous les flux RTP des sessions RTP qui partagent la même clé maîtressse.

Quand 2^48 paquets SRTP ou 2^31 paquets SRTCP ont été sécurisés avec la même clé (selon celui qui arrive en premier) la gestion de clés DOIT être invoquée pour fournir de nouvelles clés maîtressses (les clés précédemment mémorisées et utilisées NE DOIVENT PAS être utilisées à nouveau) ou la session DOIT être terminée.

Différentes sessions de supports peuvent utiliser un mélange de différents profils, en particulier incluant un profil sûr et un profil non sûr. Cependant, mélanger des sessions de supports sûres et non sûres peut révéler des informations à des tiers et donc la décision de faire ainsi DOIT être en ligne avec la politique de sécurité locale. Par exemple, la politique locale DOIT spécifier si il est acceptable d'avoir, par exemple, le flux audio non sécurisé et le flux vidéo qui s'y rapporte sécurisé.

Les considérations de sécurité de la [RFC4585] sont aussi valides. Noter en particulier, qu'appliquer le profil SAVPF implique une protection d'intégrité obligatoire sur RTCP. Bien que cela résolve le problème des faux paquets provenant de membres qui n'appartiennent pas au groupe, cela ne résout pas les problèmes relatifs au membre malveillant qui agit de façon inappropriée.

6. Considérations relatives à l'IANA

Les informations de contact suivantes devront être utilisées pour tous les enregistrements inclus ici :

Contact : Joerg Ott
mél : jo@acm.org
tél : +358-9-451-2460

Le profil de rétroaction RTP sûre, comme combinaison du profil RTP sûr et de rétroaction, a été enregistré pour le protocole de description de session (spécifiquement le type "proto") : "RTP/SAVPF".

Protocole SDP ("proto") :

Nom : RTP/SAVPF
Forme longue : Profil RTP sécurisé avec rétroaction fondée sur RTCP
Type de nom : proto
Type d'attribut : niveau supports seulement
Objet : RFC 5124
Référence : RFC 5124

Tous les attributs SDP définis pour RTP/SAVP et RTP/AVPF sont valides aussi pour RTP/SAVPF.

7. Remerciements

Le présent document a été produit par le groupe de travail Transport audio-visuel (AVT) de l'IETF. Les auteurs tiennent à remercier Magnus Westerlund, Colin Perkins, et Cullen Jennings de leurs commentaires.

8. Références

8.1 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)

[RFC2326] H. Schulzrinne, A. Rao et R. Lanphier, "Protocole de flux directs en temps réel (RTSP)", avril 1998. *(Remplacée par* RFC7826)

[RFC3264] J. Rosenberg et H. Schulzrinne, "Modèle d'offre/réponse avec le protocole de description de session (SDP)", juin 2002. *(P.S. ; MàJ par* RFC8843, 9143)

[RFC3550] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : un protocole de transport pour les applications en temps réel", STD 64, juillet 2003. *(MàJ par* RFC7164, RFC7160, RFC8083, RFC8108, RFC8860)

[RFC3551] H. Schulzrinne et S. Casner, "Profil RTP pour conférences audio et vidéo avec contrôle minimal", STD 65, juillet 2003. *(MàJ par* RFC8860)

[RFC3711] M. Baugher et autres, "Protocole de transport sécurisé en temps réel (SRTP)", mars 2004. *(P.S. ; MàJ par* RFC9335*)*

[RFC4566] M. Handley, V. Jacobson et C. Perkins, "SDP : Protocole de description de session", juillet 2006. *(P.S. ; remplacée par RFC8866)*

[RFC4567] J. Arkko et autres, "Extensions de gestion de clés pour le protocole de description de session (SDP) et le protocole d'écoulement en temps réel (RTSP)", juillet 2006. *(P.S.)*

[RFC4568] F. Andreasen et autres, "Définition d'attributs de sécurité dans le protocole de description de session (SDP) pour les flux de support", juillet 2006. *(P.S.)*

[RFC4585] J. Ott et autres, "Profil RTP étendu pour rétroaction fondée sur le protocole de contrôle de transport en temps réel (RTCP) (RTP/AVPF)", juillet 2006. *(P.S., MàJ par* RFC8108)

8.2 Références pour information

[RFC2818] E. Rescorla, "HTTP sur TLS", mai 2000. *(Information ; remplacée par* RFC9110*)*

[RFC2974] M. Handley, C. Perkins, E. Whelan, "Protocole d'annonce de session (SAP)", octobre 2000. *(Expérimentale)*

[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)

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

[RFC5764] D. McGrew, E. Rescorla, "Extension à la sécurité de la couche de transport de datagrammes (DTLS) pour établir des clés pour le protocole sécurisé de transport en temps réel (SRTP)", mai 2010. *(P. S.)*

[RFC5939] F. Andreasen, "Négociation de capacités dans le protocole de description de session (SDP)", septembre 2010. *(P.S.)*

Adresse des auteurs

Joerg Ott
Helsinki University of Technology
Otakaari 5A
FI-02150 Espoo
téléphone : +358-9-451-2460
mél : jo@comnet.tkk.fi

Elisabetta Carrara
Royal Institute of Technology
Stockholm
Sweden
mél : carrara@kth.se

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui 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.