Groupe de travail Réseau
Request for Comments : 3740
Catégorie : Information
Traduction Claude Brière de L'Isle

T. Hardjono, Verisign
B. Weis, Cisco
mars 2004

Architecture de sécurité de groupe de diffusion groupée

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

Résumé
Le présent document donne une vue d'ensemble et les raisons de l'architecture de sécurité de diffusion groupée utilisée pour sécuriser les paquets de données des grands groupes de diffusion groupée. Le document commence par introduire un cadre de référence de sécurité de la diffusion groupée, et identifie les services de sécurité qui peuvent faire partie d'une solution de diffusion groupée sûre.

Table des Matières

1 Introduction

Sécuriser la communication IP de groupe de diffusion groupée est une tâche complexe qui implique de nombreux aspects. Par conséquent, une suite sûre de protocoles de diffusion groupée IP doit avoir un certain nombre de zones fonctionnelles qui visent les différents aspects de la solution. Le présent document décrit ces zones fonctionnelles et la façon dont elles s'articulent entre elles.

1.1 Domaine d'application

Cette architecture est concernée par la sécurisation des grands groupes de diffusion groupée. Bien qu'elle puisse aussi être utilisée pour de plus petits groupes, elle n'est pas nécessairement le moyen le plus efficace. D'autres architectures (par exemple, l'architecture Cliques [STW]) peuvent être plus efficaces pour les communications de petits groupes ad hoc.

Cette architecture est "de bout en bout", et n'exige pas de protocole d'acheminement de diffusion groupée (par exemple, PIM [RFC2362]) pour participer à cette architecture. Un acheminement inapproprié peut causer un déni de service aux groupes de couche application qui se conforment à cette architecture. Cependant l'acheminement ne peut pas affecter l'authenticité ou la confidentialité des paquets de données ou de gestion du groupe. Les protocoles d'acheminement de diffusion groupée pourraient eux-mêmes utiliser cette architecture pour protéger leurs propres paquets de diffusion groupée et de groupe. Cependant, ceci serait indépendant de tout groupe sûr de couche application.

Cette architecture n'exige pas que des protocoles de contrôle d'admission de diffusion groupée IP (par exemple, IGMP [RFC3376], MLD [RFC3019]) fassent partie des groupes de diffusion groupée sécurisée. À ce titre, une opération "joindre" ou "quitter" pour un groupe sûr est indépendante d'un "joindre" ou "quitter" d'un groupe de diffusion groupée IP. Par exemple, le processus de se joindre à un groupe sûr exige d'être authentifié et autorisé par un appareil de sécurité, tandis que le processus de jonction à un groupe de diffusion groupée IP implique de contacter un routeur à capacité de diffusion groupée. Les protocoles de contrôle d'admission pourraient eux-mêmes utiliser cette architecture pour protéger leurs propres paquets de diffusion groupée. Cependant, cela serait indépendant de tout groupe de couche application sécurisée.

Cette architecture ne décrit pas explicitement comment les groupes de diffusion groupée sécurisée traitent la traduction d'adresse réseau (NAT, *Network Address Translation*) [RFC2663]. Les protocoles d'acheminement de diffusion groupée exigent généralement que les adresses et accès de source et destination d'un paquet de diffusion groupée IP restent inchangés. Cela permet de créer des arborescences de distribution de diffusion groupée cohérentes tout au long du réseau. Si un NAT est utilisé dans un réseau, la connexité des envoyeurs et des receveurs peut alors être contrariée. Cette situation n'est ni améliorée ni dégradée par suite du déploiement de cette architecture.

Cette architecture n'exige pas l'utilisation de mécanismes fiables, ni pour les protocoles de données ni pour les protocoles de gestion. L'utilisation de techniques d'acheminement de diffusion groupée fiable (par exemple, la correction d'erreur directe (FEC) [RFC3453]) améliore la disponibilité des groupes de diffusion groupée sécurisée. Cependant l'authenticité ou la confidentialité des paquets de données ou de gestion du groupe n'est pas affectée par l'omission de cette capacité dans une mise en œuvre.

1.2 Résumé du contenu du document

Le présent document donne une vue d'ensemble de l'architecture qui présente les services de sécurité exigés pour sécuriser les grands groupes de diffusion groupée. Il fournit un cadre de référence pour organiser les divers éléments au sein de l'architecture, et explique les éléments du cadre de référence.

Le cadre de référence organise les éléments de l'architecture selon trois zones fonctionnelles relevant de la sécurité. Ces éléments couvrent le traitement des données qui sont à envoyer à un groupe, la gestion du matériel de chiffrement utilisé pour protéger les données, et les politiques qui gouvernent les groupes.

Un autre élément important dans le présent document est la définition et l'explication des associations de sécurité de groupe (GSA, *Group Security Association*) qui est la contrepartie en diffusion groupée de l'association de sécurité (SA, *Security Association*) de l'envoi individuel. La GSA est spécifique de la sécurité de la diffusion groupée est c'est le fondement du travail sur le gestion de clé de groupe.

1.3 Public visé

Le présent document s'adresse à la communauté technique, aux mises en œuvre des technologies de la sécurité de la diffusion groupée IP, et à tous ceux qui s'intéressent à la compréhension des fondements généraux de la sécurité de la diffusion groupée. Le présent document suppose que le lecteur est familiarisé avec le protocole Internet, la suite des protocoles IPsec (par exemple, la [RFC2401]), la technologie de réseautage qui s'y rapporte, et avec les termes et concepts généraux de la sécurité.

1.4 Terminologie

Les termes clés suivants sont utilisés tout au long du présent document.

1-à-N
Un groupe qui a un envoyeur et de nombreux receveurs.

Association de sécurité de groupe (GSA, *Group Security Association*)
Faisceau d'associations de sécurité (SA) qui ensemble définissent comment un groupe communique en toute sécurité. La GSA peut inclure une SA de protocole d'enregistrement, une SA de protocole de changement de clés, et une ou plusieurs SA de protocole de sécurité des données.

M-à-N
Groupe qui a de nombreux envoyeurs et de nombreux receveurs, où M et N ne sont pas nécessairement de la même valeur.

Association de sécurité (SA, *Security Association*)
Ensemble de politiques et de clés cryptographiques qui fournit des services de sécurité au trafic réseau qui satisfait à cette politique.

2. Conception de l'architecture : cadre de référence de sécurité de diffusion groupée

Cette section examine les questions complexes de la sécurité de la diffusion groupée dans le contexte d'un cadre de référence. Ce cadre de référence est utilisé pour classer les zones fonctionnelles, les éléments fonctionnels, et les interfaces. On montre deux conceptions de ce cadre de référence : une conception centralisée, et une conception répartie qui étend la conception centralisée pour les très grands groupes.

2.1 Cadre de référence

Le cadre de référence se fonde sur trois grandes zones fonctionnelles (comme le montre la Figure 1). Le cadre de référence incorpore les principales entités et fonctions qui se rapportent à la sécurité de la diffusion groupée, et décrit leurs interrelations. Il exprime aussi la sécurité de la diffusion groupée dans la perspective des types de groupes de diffusion groupée (1-à-N et M-à-N) et des classes de protocoles (les messages échangés) nécessaires pour sécuriser les paquets de diffusion groupée.

Le but du cadre de référence est de fournir un contexte général autour des zones fonctionnelles, et les relations entre les zones fonctionnelles. Noter que certains problèmes s'étendent sur plus d'une zone fonctionnelle. En fait, le cadre encourage l'identification et la formulation précise des questions qui impliquent plus d'une zone fonctionnelle ou celles qui sont difficiles à exprimer dans les termes d'une seule zone fonctionnelle. Un exemple d'un tel cas est l'expression des politiques qui concernent les clés de groupe, qui impliquent les zones fonctionnelles à la fois de la gestion de clé de groupe et des politiques de diffusion groupée.

Quand on examine les diagrammes du cadre de référence, il est important de comprendre que les "boîtes" individuelles dans le cadre n'impliquent pas nécessairement qu'une entité individuelle correspondante mette en œuvre une certaine fonction. Une boîte dans le cadre devrait plutôt être interprétée comme relevant d'une façon lâche d'une certaine fonction relative à une zone fonctionnelle. Que cette fonction soit en réalité mise en œuvre comme une ou plusieurs entités physiques dépend de la solution particulière. Par exemple, la boîte marquée "Serveur de clé" doit être interprétée au sens large comme se référant aux fonctions de gestion de clé.

De même, le cadre de référence rend compte de certaines mises en œuvre qui peuvent en fait fusionner un certain nombre des "boîtes" en une seule entité physique. Ceci pourrait être vrai même à travers des zones fonctionnelles. Par exemple, une entité dans un groupe pourrait agir à la fois comme contrôleur de groupe et comme envoyeur à un groupe.

Les protocoles à normaliser sont décrits dans les diagrammes du cadre de référence par les flèches qui connectent les diverses boîtes. La Section 4 donne plus de détails.

2.2 Éléments du cadre de référence centralisé

Le diagramme du cadre de référence de la Figure 1 contient des boîtes et des flèches. Les boîtes sont les entités fonctionnelles et les flèches sont les interfaces entre elles. Des protocoles standard sont nécessaires pour les interfaces, qui prennent en charge les services de diffusion groupée entre les entités fonctionnelles.

Dans certains cas, un système qui met en œuvre l'architecture de sécurité de la diffusion groupée peut n'avoir pas besoin de mettre en œuvre des protocoles pour prendre en compte chaque interface. Ces interfaces peuvent être plutôt satisfaites par l'utilisation d'une configuration manuelle, ou même omises si elles ne sont pas nécessaires pour l'application.

Il y a trois ensembles d'entités fonctionnelles. Chacun est exposé ci-dessous.

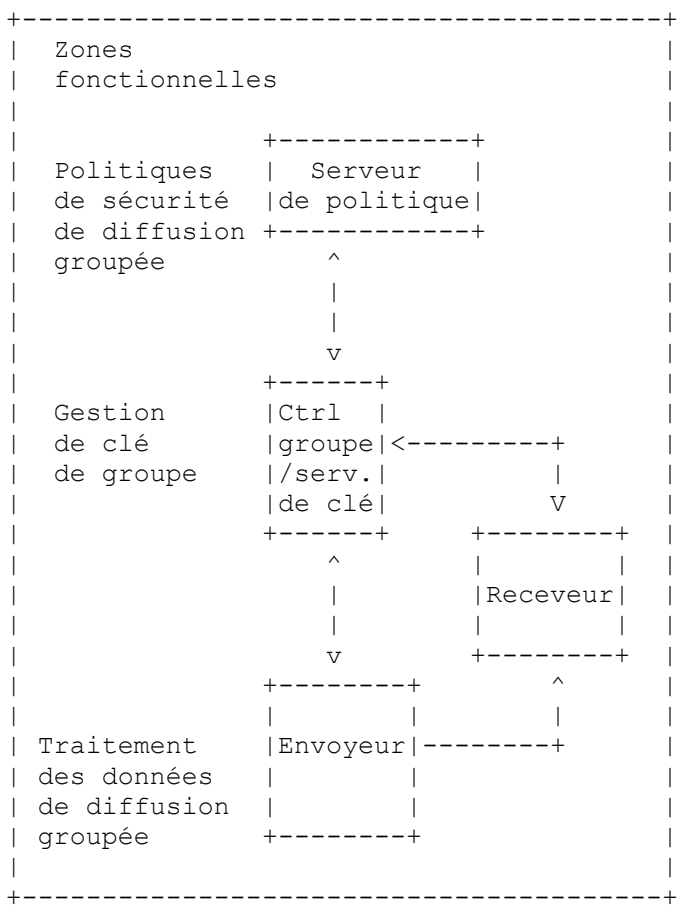

Figure 1 : Cadre de référence de sécurité centralisée de diffusion groupée

2.2.1 Contrôleur de groupe et serveur de clés

Le contrôleur de groupe et serveur de clés (GCKS, *Group Controller and Key Server*) représente à la fois l'entité et les fonctions qui se rapportent à la production et à la gestion des clés de chiffrement utilisées par un groupe de diffusion groupée. Le GCKS effectue aussi les vérifications d'authentification et d'autorisation de l'utilisateur sur les candidats membres du groupe de diffusion groupée.

Le serveur de clés (KS, *Key Server*) et le contrôleur de groupe (GC, *Group Controller*) ont des fonctionnalités quelque peu différentes et peuvent en principe être considérés comme des entités distinctes. Actuellement; le cadre considère les deux entités comme une "boîte" afin de simplifier la conception, et afin de ne pas rendre obligatoire la normalisation du protocole entre le KS et le GC. On souligne que le KS et le GC n'ont pas besoin de cohabiter. De plus, de futures conceptions peuvent choisir de normaliser le protocole entre GC et KS, sans altérer les autres composants.

2.2.2 Envoyeur et receveur

L'envoyeur est une entité qui envoie les données au groupe de diffusion groupée. Dans un groupe de diffusion groupée 1-à-N un seul envoyeur est autorisé à transmettre des données au groupe. Dans un groupe de diffusion groupée M-à-N, deux membres du groupe ou plus sont autorisés à être des envoyeurs. Dans certains groupes, tous les membres sont des envoyeurs autorisés.

Envoyeurs et receveurs doivent tous deux interagir avec l'entité GCKS pour les besoins de la gestion de clés. Cela inclut l'authentification de l'utilisateur et/ou de l'appareil, l'autorisation de l'utilisateur et/ou de l'appareil, l'obtention du matériel de chiffrement en accord avec des politiques de gestion de clé pour le groupe, l'obtention de nouvelles clés durant les mises à jour de clés, et l'obtention d'autres messages se rapportant à la gestion du matériel de chiffrement et des paramètres de sécurité.

Envoyeurs et receveurs peuvent recevoir beaucoup de leur politique des entités GCKS. L'événement de jonction à un groupe de diffusion groupée est normalement couplé avec l'obtention par l'envoyeur/receveur du matériel de chiffrement d'une entité GCKS. Ceci n'empêche pas l'interaction directe entre l'envoyeur/receveur et le serveur de politique.

2.2.3 Serveur de politique

Le serveur de politique représente à la fois l'entité et les fonctions utilisées pour créer et gérer les politiques de sécurité spécifiques d'un groupe de diffusion groupée. Le serveur de politique interagit avec l'entité GCKS afin d'installer et gérer les politiques de sécurité relatives à l'adhésion à un certain groupe de diffusion groupée et celles relatives au matériel de chiffrement pour un groupe de diffusion groupée.

Les interactions entre le serveur de politique et les autres entités dans le cadre de référence dépendent dans une large mesure des circonstances de sécurité visées par une certaine politique.

2.3 Éléments du cadre de référence réparti

Le besoin d'adaptabilité des solutions aux grands groupes à travers des régions géographiques larges dans l'Internet exige que les éléments du cadre de référence fonctionnent aussi comme un système réparti. La Figure 2 montre comment le concept de répartition de la prise en charge de l'adaptation à de grands groupes rentre dans le cadre de référence.

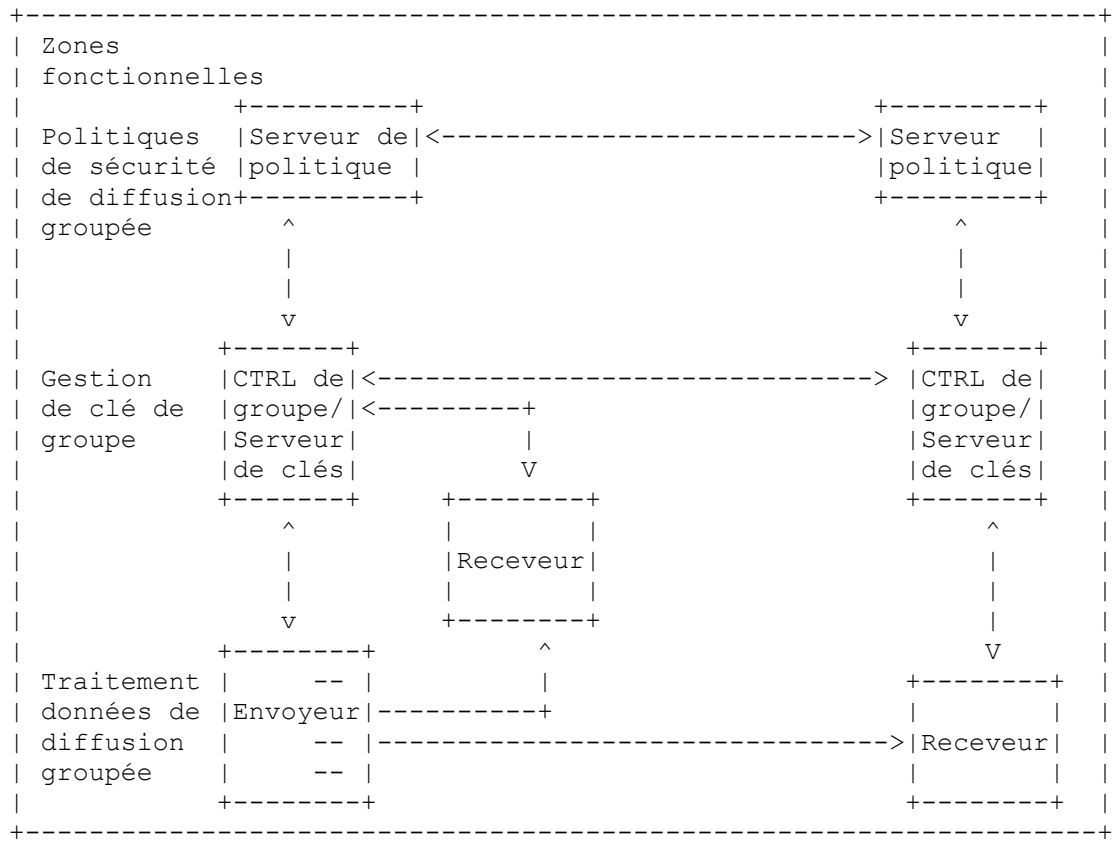

Figure 2 : Cadre de référence de sécurité répartie de diffusion groupée

Dans une conception répartie, l'entité GCKS interagit avec les autres entités GCKS pour réaliser l'adaptabilité des services relatifs à la gestion de clé. Les entités GCKS vont avoir besoin d'un moyen d'authentifier leurs entités GCKS homologues, d'un moyen pour autoriser, et d'un moyen d'interagir en toute sécurité pour passer les clés et la politique.

De façon similaire, les serveurs de politique doivent interagir les uns avec les autres en toute sécurité pour permettre la communication et la mise en application des politiques à travers l'Internet.

Deux boîtes Receveur sont affichées qui correspondent respectivement à la situation où l'envoyeur et le receveur emploient tous deux la même entité GCKS (architecture centralisée) et à celle où l'envoyeur et le receveur emploient des entités GCKS différentes (architecture répartie). Dans la conception répartie, tous les receveurs doivent obtenir des clés et politiques identiques. Chaque membre d'un groupe de diffusion groupée peut interagir avec une entité GCKS principale (par exemple, l'entité GCKS "la plus proche", mesurée dans les termes d'une métrique bien définie et cohérente). De façon similaire, une entité GCKS peut interagir avec un ou plusieurs serveurs de politique, aussi rangés dans une architecture répartie.

3. Zones fonctionnelles

Le cadre de référence identifie trois zones fonctionnelles. Ce sont :
- Le traitement des données de diffusion groupée. Cette zone couvre les traitements en rapport avec la sécurité des données de diffusion groupée de la part de l'envoyeur et des receveurs. Cette zone fonctionnelle est exposée au paragraphe 3.1.
- La gestion de clé de groupe. Cette zone est concernée par la distribution sûre et le rafraîchissement du matériel de chiffrement. Cette zone fonctionnelle est exposée au paragraphe 3.2.
- Les politiques de sécurité de diffusion groupée. Cette zone couvre les aspects de la politique dans le contexte de la sécurité de la diffusion groupée, en prenant en considération le fait que les politiques peuvent être exprimées de différentes façons : elles peuvent exister à différents niveaux dans une certaine architecture de sécurité de la diffusion groupée, et elles peuvent être interprétées différemment selon le contexte dans lequel elles sont spécifiées et mises en œuvre. Cette zone fonctionnelle est exposée au paragraphe 3.3.

3.1 Traitement des données de diffusion groupée

Dans un groupe de diffusion groupée sûre, les données normalement nécessaires sont :
1. Chiffrées en utilisant la clé de groupe, principalement pour le contrôle d'accès et éventuellement aussi pour la confidentialité.
2. Authentifiées, pour vérifier la source et l'intégrité des données. L'authentification prend deux formes :
   a. Authentification de la source et intégrité des données. Cette fonctionnalité garantit que les données ont été générées par la source prétendue et n'ont pas été modifiées en route (soit par un membre du groupe, soit par un attaquant externe).
   b. Authentification de groupe. Ce type d'authentification garantit seulement que les données ont été générées (ou modifiées pour la dernière fois) par un membre du groupe. Elle ne garantit pas l'intégrité des données sauf si tous les membres du groupe sont de confiance.

Tandis que le chiffrement et l'authentification de groupe dans la diffusion groupée sont très standard et similaires au chiffrement et à l'authentification d'une communication point à point, l'authentification de la source pour la diffusion groupée est considérablement plus compliquée. Par conséquent, les solutions toutes faites (par exemple, tirées de IPsec [RFC2406]) peuvent être suffisantes pour le chiffrement et l'authentification de groupe, mais pour l'authentification de source, des transformations particulièrement adaptées sont nécessaires. Voir dans [CCPRRS] des développements complémentaires sur les problèmes qui concernent les transformations de données.

Les données de diffusion groupée chiffrées et/ou authentifiées par un envoyeur devraient être traitées de la même façon par les receveurs des conceptions centralisée et répartie (comme le montre la Figure 2).

La "diffusion groupée encapsulant une charge utile de sécurité" [BCCR] donne la définition de ESP en diffusion groupée pour le trafic de données. La spécification de la transformation d'authentification de source de diffusion groupée [RFC4082] définit l'utilisation de l'algorithme TESLA pour l'authentification de la source dans la diffusion groupée.

3.2 Gestion de clé de groupe

Le terme de "matériel de chiffrement" se réfère aux clés de chiffrement qui appartiennent à un groupe, à l'état associé aux clés,

et aux autres paramètres de sécurité qui se rapportent aux clés. Donc, la gestion des clés de chiffrement qui appartiennent à un groupe exige nécessairement la gestion de leur état et des paramètres associés. Des solutions à ces questions spécifiques doivent être proposées. Cela peut inclure :

- les méthodes d'identification et d'authentification des membres
- les méthodes pour vérifier les membres des groupes
- les méthodes d'établissement d'un canal sûr entre une entité GCKS et le membre, afin de livrer du matériel de chiffrement à plus court terme relevant d'un groupe
- les méthodes pour établir un canal sûr à long terme entre une entité GCKS et une autre, afin de distribuer du matériel de chiffrement à plus court terme relevant d'un groupe
- les méthodes pour effectuer le changement des clés et du matériel de chiffrement
- les méthodes pour détecter et signaler les défaillances et les compromissions perçues des clés et du matériel de chiffrement.

Les exigences relatives à la gestion du matériel de chiffrement doivent être vues dans le contexte des politiques qui s'imposent dans les circonstances données.

La gestion de l'association de sécurité est au cœur de la zone de gestion de clés, et elles sera exposée plus loin.

Le document "Architecture de gestion de clé de groupe" [RFC4046] définit plus en détails l'architecture de gestion de clés pour la sécurité de la diffusion groupée. Il s'élabore sur le concept de l'association de sécurité de groupe (GSA) et définit plus précisément les rôles du serveur de clés et du contrôleur de groupe.

"Interprétation du domaine de groupe" [RFC3547], "GSAKMP" [RFC4535], et "MIKEY" [RFC3830] sont trois instances de protocoles qui mettent en œuvre la fonction de gestion de clé de groupe.

3.3 Politiques de sécurité de diffusion groupée

Les politiques de sécurité de diffusion groupée doivent fournir les règles de fonctionnement des autres éléments du cadre de référence. Les politiques de sécurité peuvent être distribuées de façon ad hoc dans certaines instances. Cependant, une meilleure coordination et de plus hauts niveaux de garantie sont obtenus si un contrôleur de politique distribue la politique de sécurité dans le groupe.

Les politiques de sécurité de diffusion groupée doivent représenter, ou contenir, plus d'informations qu'une politique traditionnelle d'homologue à homologue. En plus de représenter les mécanismes de sécurité pour la communication de groupe, la politique doit aussi représenter les règles du gouvernement du groupe sûr. Par exemple, la politique va spécifier le niveau d'autorisation nécessaire pour qu'une entité se joigne à un groupe. Des opérations plus avancées vont inclure les conditions suivant lesquelles un membre du groupe sera forcément retiré du groupe, et quoi faire si les membres du groupe ont besoin de se resynchroniser à cause de la perte de messages de gestion de clé.

L'application de la politique à l'élément contrôleur de groupe et aux éléments membres (envoyeur et receveur) doit être décrite. Bien qu'il y ait déjà une base pour la gestion de la politique de sécurité dans l'IETF, la gestion de la politique de sécurité de la diffusion groupée étend les concepts développés pour la communication en envoi individuel dans les domaines de :

- la création de politique,
- la traduction de politique de haut niveau,
- la représentation de la politique.

Les exemples des travaux sur les politiques de sécurité de la diffusion groupée incluent le projet de gestion dynamique de contexte cryptographique [Din], le protocole de gestion de clé de groupe [RFC2093], [RFC2094], et Antigone [McD].

La création de politique pour une diffusion groupée sécurisée a plusieurs dimensions de plus que le seul administrateur spécifié dans la politique supposée dans les cadres existants de politique d'envoi individuel. Les groupes de diffusion groupée sécurisée sont généralement grands et par leur nature même s'étendent sur plusieurs domaines administratifs, quand ils ne s'étendent pas sur un domaine différent pour chaque utilisateur. Il y a plusieurs méthodes qui doivent être examinées pour la création d'une seule politique de sécurité de groupe cohérente. Elles incluent une spécification de haut en bas de la politique de groupe de l'initiateur du groupe et la négociation de la politique entre les membres du groupe (ou les candidats membres). La négociation peut être aussi simple qu'une stricte intersection des politiques des membres ou extrêmement compliquée en utilisant des systèmes de vote pondéré.

La traduction des règles de politique d'un modèle de données en un autre est beaucoup plus difficile dans un environnement de groupe de diffusion groupée. Ceci est particulièrement vrai lorsque l'appartenance au groupe s'étend sur de nombreux domaines administratifs. Les politiques spécifiées à haut niveau avec un outil de gestion de politique doivent être traduites en

règles plus précises que ce que les mécanismes disponibles de politique de sécurité peuvent à la fois comprendre et mettre en œuvre. Quand on traite de communications en diffusion groupée et de leurs multiples participants, il est essentiel que la traduction individuelle effectuée pour chaque participant résulte en l'utilisation d'un mécanisme qui soit interopérable avec les résultats de toutes les autres traductions. Normalement, la traduction de la politique de haut niveau en objets de politique spécifiques doit résulter en les mêmes objets afin de réaliser la communication entre tous les membres du groupe. L'exigence que la traduction de politique résulte en les mêmes objets fait peser des contraintes sur l'utilisation et les représentations des politiques de haut niveau.

Il est aussi important que la négociation et la traduction de la politique soient effectuées comme parties intégrantes de l'adhésion à un groupe. Ajouter un membre à un groupe n'a pas de sens si il n'est pas capable de participer aux communications du groupe.

4. Associations de sécurité de groupe (GSA)

4.1 Association de sécurité

Une association de sécurité est un terme couramment utilisé dans les systèmes cryptographiques (par exemple, [RFC2401], [RFC2409], [RFC4303]). Le présent document utilise le terme pour désigner tout ensemble de politique et de clés de chiffrement qui fournit des services de sécurité pour le trafic réseau qui satisfait à cette politique. Une association de sécurité contient généralement les attributs suivants :

- des sélecteurs, comme des adresses de transport de source et de destination,
- des propriétés, comme un indice de paramètre de sécurité (SPI) ou une paire de mouchards, et des identités,
- une politique de chiffrement, comme les algorithmes, les modes, les durées de vie des clés, et les longueurs de clé utilisées pour l'authentification ou la confidentialité,
- des clés, comme les clés d'authentification, de chiffrement et de signature.

La gestion de clé de groupe utilise un ensemble différent d'abstractions que les systèmes de gestion de clé point à point (comme IKE [RFC2409]). Néanmoins, les abstractions utilisées dans la zone fonctionnelle de gestion de clé de groupe peuvent être construites à partir des abstractions de gestion de clé point à point.

4.2 Structure d'une GSA : Introduction

Les associations de sécurité (SA) pour la gestion de clé de groupe sont plus complexes, et généralement plus nombreuses que dans les algorithmes de gestion de clé point à point. Ces dernières établissent une SA de gestion de clé pour protéger des SA d'application (généralement une ou deux selon le protocole). Cependant, la gestion de clé de groupe peut exiger jusqu'à trois SA ou plus. Ces SA sont décrites dans les paragraphes qui suivent.

Une GSA contient tous les attributs de la SA identifiés dans la section précédente, ainsi que certains attributs supplémentaires relevant du groupe. Comme le montre la Figure 3, la GSA se construit sur la SA de deux manières distinctes.

- D'abord, la GSA est un sur ensemble de SA (Figure 3(a)). Une GSA a des attributs de politique de groupe. Par exemple, la sorte d'accréditifs signés nécessaires pour l'adhésion au groupe, si les membres du groupe reçoivent de nouvelles clés lorsque un membre est ajouté (ce qu'on appelle plus loin "rétro changement de clé") ou si les membres du groupe vont recevoir de nouvelles clés lorsque un membre est retiré du groupe ("changement de clé vers l'avant"). Une GSA inclut aussi une SA comme attribut d'elle-même.
- Ensuite, la GSA est une agrégation de SA (Figure 3(b)). Une GSA est composée de multiples SA, et ces SA peuvent être utilisées à plusieurs fins indépendantes.

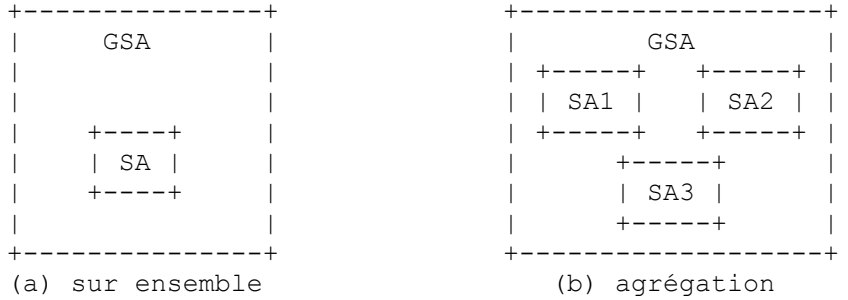

Figure 3 : Relations de GSA à SA

4.3 Structure d'une GSA : Raisonnement

La Figure 4 montre trois catégories de SA qui peuvent être agrégées en une GSA.

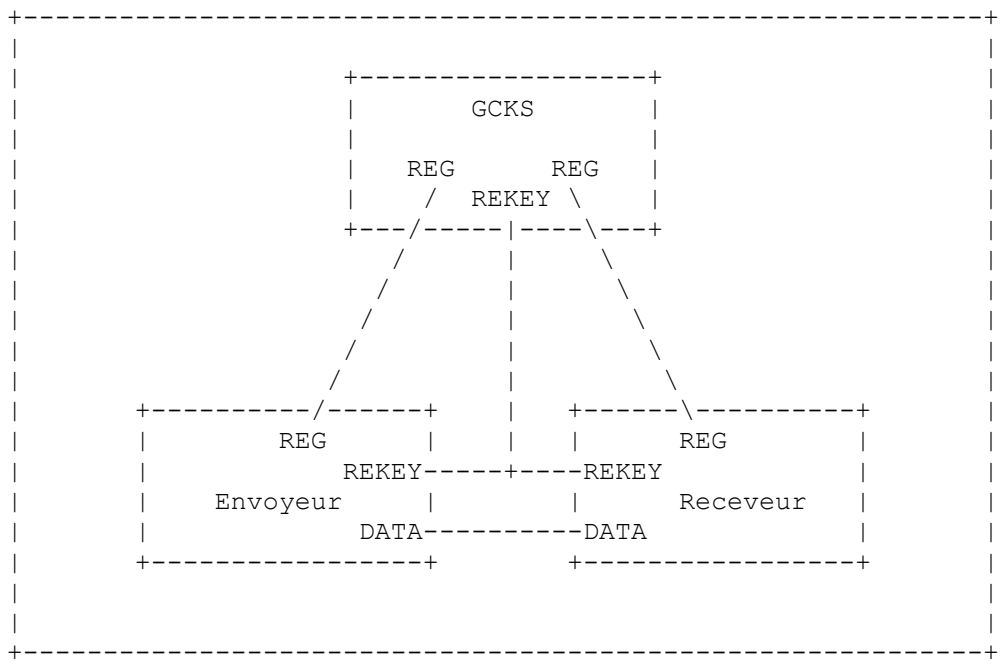

Figure 4 : Structure de GSA et trois catégories de SA

Les trois catégories de SA sont :
- SA d'enregistrement (REG) : c'est une SA séparée entre le GCKS et chaque membre du groupe, sans considération de son statut d'envoyeur, de receveur ou s'il agit dans les deux rôles.
- SA de changement de clé (REKEY) : c'est une seule SA de diffusion groupée entre le GCKS et tous les membres du groupe.
- SA de sécurité des données (DATA) : c'est une SA de diffusion groupée entre chaque source de diffusion groupée et les receveurs du groupe. Il peut y avoir autant de SA de données qu'il y a de sources de diffusion groupée permises par la politique du groupe.

Chacune de ces SA est définie plus en détails au paragraphe suivant.

4.4 Définition de la GSA

Les trois catégories de SA correspondent aux trois différentes sortes de communications couramment exigées pour les communications de groupe. Ce paragraphe décrit en détails les SA qui apparaissent à la Figure 4.

- SA d'enregistrement (REG) :

Une SA est nécessaire pour les communications en envoi individuel (bidirectionnelles) entre le GCKS et un membre du groupe (qu'il soit envoyeur ou receveur). Cette SA n'est établie qu'entre le GCKS et un membre. L'entité GCKS est chargée du contrôle d'accès aux clés du groupe, avec la distribution de la politique aux membres (ou candidats membres) et de la dissémination des clés de groupe aux membres envoyeurs et receveurs. Cette utilisation d'une SA (en envoi individuel) comme point de départ de la gestion de clés est commun à un certain nombre d'environnements de gestion de clés de groupe [RFC3547], [RFC4535], [CCPRRS], [RFC2627], [BMS].

La SA d'enregistrement est initiée par le membre pour tirer les informations de la GSA du GCKS. C'est comme cela que se font les demandes d'adhésion au groupe sécurisé, ou que sont réinitialisées les clés de GSA après avoir été déconnecté du groupe (par exemple, quand l'ordinateur hôte a été éteint pendant les opérations de changement de clé). Les informations de GSA tirées du GCKS se rapportent aux deux autres SA définies au titre de la GSA.

Noter que cette SA (en envoi individuel) est utilisée pour protéger les autres éléments de la GSA. À ce titre, la SA

d'enregistrement est cruciale et est inséparable des deux autres SA dans la définition d'une GSA.

Cependant, l'exigence d'une SA d'enregistrement n'implique pas le besoin d'un protocole d'enregistrement pour créer cette SA d'enregistrement. Elle pourrait être plutôt établie par les mêmes moyens manuels comme la distribution sur une carte à mémoire. Donc, ce qui importe est qu'une SA d'enregistrement existe, et soit utilisée pour protéger les autres SA.

Du point de vue d'un GCKS, il y a autant de SA d'enregistrement uniques qu'il y a de membres (envoyeurs et/ou receveurs) dans le groupe. Cela peut constituer un problème d'adaptabilité pour certaines applications. Une SA d'enregistrement peut être établie à la demande avec une courte durée de vie, tandis que des SA de changement de clé et de sécurité des données sont établies au moins pour la durée des sessions qu'elles prennent en charge.

À l'inverse, les SA d'enregistrement pourraient être laissées en place pour la durée de vie du groupe, si l'adaptabilité ne pose pas de problème. Une telle SA d'enregistrement de long terme serait utile pour les besoins de resynchronisation ou de désenregistrement.

- SA de changement de clé (REKEY) :

Dans certains cas, un GCKS a besoin de la capacité de "pousser" de nouvelles SA au titre de la GSA. Ces nouvelles SA doivent être envoyées à tous les membres du groupe. Dans d'autres cas, le GCKS a besoin de la capacité de révoquer rapidement l'accès à un ou plusieurs membres du groupe. Ces deux besoins sont satisfaits par la SA de changement de clés.

Cette SA de changement de clés est une transmission unidirectionnelle en diffusion groupée des messages de gestion de clé à partir du GCKS à tous les membres du groupe. À ce titre, cette SA est connue par le GCKS et par tous les membres du groupe.

Cette SA n'est pas négociée, car tous les membres du groupe doivent la partager. Donc, le GCKS doit être la source authentique et agir comme seul point de contact pour les membres du groupe pour obtenir cette SA.

Il n'est absolument pas exigé qu'une SA de changement de clés fasse partie d'une GSA. Par exemple, la durée de vie de certains groupes peut être assez brève pour qu'un changement de clés ne soit pas nécessaire. À l'inverse, la politique pour le groupe pourrait spécifier plusieurs SA de changement de clés de différents types. Par exemple, si le GC et le KS sont des entités séparées, le GC peut délivrer des messages de changement de clés qui s'ajustent à l'appartenance au groupe, et le KS peut délivrer des messages de changement de clés aux nouvelles SA de données.

- SA de sécurité des données (DATA) :

La SA de sécurité des données protège les données entre les membres envoyeurs et les membres receveurs. Une ou plusieurs SA sont nécessaires pour la transmission en diffusion groupée des messages de données de l'envoyeur aux autres membres du groupe. Cette SA est connue par le GCKS et par tous les membres du groupe.

Sans considération du nombre d'instances de cette troisième catégorie de SA, cette SA n'est pas négociée. Tous les membres du groupe l'obtiennent du GCKS. Le GCKS lui-même n'utilise pas cette catégorie de SA.

Du point de vue des receveurs, il y a au moins une SA de sécurité des données pour le membre envoyeur (un ou plusieurs) dans le groupe. Si le groupe a plus d'une SA de sécurité des données, le protocole de sécurité des données doit avoir un moyen de différencier les SA (par exemple, avec un indice de paramètre de sécurité (SPI)).

Il y a un certain nombre de possibilités quant au nombre de SA de sécurité des données :

1. Chaque envoyeur dans le groupe pourrait recevoir une SA de sécurité des données unique, d'où il résulte que chaque receveur devra entretenir autant de SA de sécurité des données qu'il y a d'envoyeurs dans le groupe. Dans ce cas, chaque envoyeur peut être vérifié en utilisant les techniques d'authentification d'origine de la source.
2. Le groupe entier déploie une seule SA de sécurité des données pour tous les envoyeurs. Les receveurs vont alors être capables d'entretenir seulement une SA de sécurité des données.
3. Une combinaison de 1. et 2.

4.5 Compositions normales de GSA

Selon la politique du groupe de diffusion groupée, de nombreuses compositions d'une GSA sont possibles. Pour illustrer cela, ce paragraphe décrit quelques compositions possibles :

- Un groupe de membres avec des contraintes de mémoire peut requérir une seule SA REG, et une seule SA DATA.
- Une application de "session à la demande", où toutes les informations de SA nécessaires pour la session peuvent être distribuées sur une SA REG. Les SA de changement de clé et de réinitialisation des SA DATA peuvent n'être pas nécessaires, de sorte qu'il n'y a pas de SA REKEY.
- Un groupe par abonnement, où le matériel de chiffrement est changé lorsque les membres changent. Une SA REG est

nécessaire pour distribuer les autres SA ; une SA REKEY est nécessaire pour réinitialiser une SA DATA au moment où les membres changent.

5. Services de sécurité

Cette section identifie les services de sécurité pour les interfaces désignées sur la Figure 2. Des services de sécurité distincts sont alloués à des interfaces spécifiques. Par exemple, l'authentification de la source de la diffusion groupée, l'authentification des données, et la confidentialité se produisent sur l'interface de données de diffusion groupée entre les envoyeurs et les receveurs de la Figure 2. Les services d'authentification et de confidentialité peuvent aussi être nécessaires entre le serveur de clés et les membres du groupe (c'est-à-dire, les envoyeurs et les receveurs de la Figure 2) mais les services qui sont nécessaires pour la gestion de clés de diffusion groupée peuvent être en envoi individuel aussi bien qu'en diffusion groupée. Un service de sécurité dans le cadre de référence de sécurité de diffusion groupée identifie donc une fonction spécifique le long d'une ou plusieurs interfaces de la Figure 2.

Le présent mémoire ne tente pas d'analyser les relations de confiance, les exigences fonctionnelles détaillées, les exigences de performances, les algorithmes convenables, ni les spécifications de protocoles pour la diffusion groupée IP et la sécurité de la diffusion groupée de couche application. Ce travail sera plutôt effectué lors de la définition plus précise des services de sécurité dans la réalisation des algorithmes et protocoles.

5.1 Confidentialité des données de diffusion groupée

Ce service de sécurité traite le chiffrement des données de diffusion groupée du côté de l'envoyeur et le déchiffrement des données du côté du receveur. Ce service de sécurité peut aussi s'appliquer au matériel de chiffrement qui est fourni par la gestion des clés de diffusion groupée conformément à la gestion de politique de diffusion groupée, mais il est indépendant de l'un et l'autre.

Une part importante du service de sécurité de confidentialité des données de diffusion groupée est dans l'identification et la motivation des chiffrements spécifiques qui devraient être utilisés pour les données de diffusion groupée. Évidement, tous les chiffrements ne conviennent pas pour la diffusion groupée IP et le trafic de diffusion groupée de couche application. Comme ce trafic va habituellement être des flux UDP sans connexion, les chiffrements de flux peuvent ne pas convenir, bien que des chiffrements hybrides flux/bloc puissent présenter des avantages sur certains chiffrements de bloc.

Concernant la diffusion groupée à la couche application, il convient de prendre en considération les effets de l'envoi de données chiffrées dans un environnement de diffusion groupée qui n'aurait pas de contrôle d'admission, où pratiquement tous les programmes d'application pourraient se joindre à un événement de diffusion groupée indépendamment de sa participation à un protocole de sécurité de la diffusion groupée. Donc, ce service de sécurité est aussi concerné par les effets des services de confidentialité de la diffusion groupée (volontaire ou non) sur les programmes d'application. Les effets sont considérés aussi bien sur les envoyeurs que sur les receveurs.

Dans la Figure 2, le service sécurité de confidentialité des données de diffusion groupée est placé dans la zone de traitement des données de diffusion groupée avec l'interface entre envoyeurs et receveurs. Les algorithmes et protocoles qui sont réalisés à partir du travail sur ce service de sécurité peuvent s'appliquer aux autres interfaces et zones de la Figure 2 lorsque la confidentialité des données de diffusion groupée est nécessaire.

5.2. Authentification et intégrité des données de source de diffusion groupée

Ce service de sécurité traite l'authentification de la source et la vérification de l'intégrité des données de la diffusion groupée. Cela inclut les transformations à faire aussi bien à l'extrémité d'envoi qu'à l'extrémité de réception. Cela suppose que la signature appropriée et les clés de vérification sont fournies via la gestion de clés de diffusion groupée conformément à la gestion de politique de diffusion groupée décrite plus loin. C'est une des zone de sécurité de la diffusion groupée les plus difficiles à cause de l'absence de connexion et des exigences de temps réel de beaucoup d'applications de diffusion groupée IP. Il y a cependant des classes de sécurité de la diffusion groupée de couche application où l'authentification hors ligne de la source et des données vont suffire. Comme exposé précédemment, toutes les applications de diffusion groupée n'exigent pas l'authentification en temps réel et la vérification de l'intégrité des paquets de données. Une solution robuste à l'authentification de la source et des données de diffusion groupée est cependant nécessaire pour une solution complète de la sécurité de la diffusion groupée.

Dans la Figure 2, le service de sécurité d'authentification de la source et des données de diffusion groupée est placé dans la

zone Traitement des données de diffusion groupés avec l'interface entre envoyeurs et receveurs. Les algorithmes et protocoles qui sont produits pour cette zone fonctionnelle peuvent être applicables à des services de sécurité dans d'autres zones fonctionnelles qui utilisent les services de diffusion groupée comme la gestion de clés de groupe.

5.3 Authentification de groupe de diffusion groupée

Ce service de sécurité fournit une vérification limitée de l'authenticité des données transmises : il ne garantit que les données générées par (ou modifiée en dernier par) un des membres du groupe. Il ne garantit pas l'authenticité des données dans le cas où d'autres membres du groupe ne sont pas de confiance.

L'avantage de l'authentification de groupe est qu'elle est garantie via des transformations cryptographiques relativement simples et efficaces. Donc, lorsque l'authentification de source n'est pas extraordinaire, l'authentification de groupe devient utile. De plus, effectuer l'authentification de groupe est utile même lorsque l'authentification de source est effectuée ultérieurement : elle fournit une vérification simple d'intégrité faible qui est utile comme mesure contre les attaques de déni de service.

Le service de sécurité Authentification de groupe de diffusion groupée est placé dans la zone Traitement des données de diffusion groupée avec l'interface entre envoyeurs et receveurs.

5.4 Gestion des membres du groupe de diffusion groupée

Ce service de sécurité décrit les fonctions d'enregistrement des membres auprès du contrôleur de groupe, et le désenregistrement des membres auprès du contrôleur de groupe. Ce sont des fonctions de sécurité, qui sont indépendantes des opérations de groupe de diffusion groupée IP "joindre" et "quitter" que les membre peuvent avoir besoin d'effectuer au titre des protocoles de contrôle d'admission de groupe (c'est-à-dire, IGMP [RFC3376], MLD [RFC3019]).

L'enregistrement inclut l'authentification des membres, la notification et la négociation des paramètres de sécurité, et l'enregistrement des informations selon les politiques du contrôleur de groupe et des postulants membres. (Normalement, une annonce hors bande des informations de groupe va se produire avant que l'enregistrement ait lieu. Le processus d'enregistrement sera normalement invoqué par le membre postulant.)

Le désenregistrement peut se produire soit à l'initiative du membre, soit à l'initiative du contrôleur de groupe. Il va en résulter l'enregistrement de l'événement de désenregistrement par le contrôleur de groupe et en une invocation du mécanisme approprié pour terminer l'adhésion du membre qui se désenregistre (voir le paragraphe 5.5).

Ce service de sécurité décrit aussi la fonctionnalité de communication relative à l'appartenance au groupe parmi les différents serveurs GCKS dans une conception de groupe réparti.

Dans la Figure 2, le service de sécurité Membres du groupe de diffusion groupée est placé dans la zone Gestion de clé de groupe et a des interfaces avec les envoyeurs et les receveurs.

5.5 Gestion des clés de diffusion groupée

Ce service de sécurité décrit les fonctions de distribution et de mise à jour du matériel de chiffrement tout au long de la vie du groupe. Les composants de ce service de sécurité peuvent inclure :

- une notification du GCKS aux membres du groupe (envoyeur ou receveurs) concernant le matériel de chiffrement actuel (par exemple, les clés de chiffrement et d'authentification de groupe, les clés auxiliaires utilisées pour la gestion du groupe, les clés pour l'authentification de la source, etc.)
- la mise à jour du matériel de chiffrement actuel, selon les circonstances et les politiques,
- la terminaison des groupes d'une manière sûre, incluant le groupe sûr lui-même et le matériel de chiffrement associé.

Parmi les responsabilités de ce service de sécurité figure la gestion sûre des clés entre serveurs de clés et membres du groupe, les questions d'adressage pour la distribution en diffusion groupée du matériel de chiffrement, et l'adaptabilité ou les autres exigences de performances pour la gestion des clés de diffusion groupée [RFC2627], [BMS]. Les serveurs de clés et les membres du groupe peuvent tirer parti d'une infrastructure de clé publique (PKI , *Public Key Infrastructure*) commune pour une adaptabilité accrue de l'authentification et l'autorisation.

Pour permettre un protocole interopérable et sûr de sécurité de diffusion groupée IP, ce service de sécurité peut avoir besoin de spécifier des abstractions d'hôte telles qu'une base de données d'association de sécurité de groupe (GSAD, *Group Security*

Association Database) et une base de données de politique de sécurité de groupe (GSPD, *Group Security Policy Database*) pour la sécurité de la diffusion groupée IP. Le degré de recouvrement entre la diffusion groupée IP et la gestion de clé de couche application doit être pris en compte. Donc, ce service de sécurité prend en compte les exigences de la gestion de clés pour la diffusion groupée IP, les exigences de gestion de clé pour la diffusion groupée à la couche application, et le degré auquel les réalisations spécifiques d'un service de sécurité de gestion de clés de diffusion groupée peuvent satisfaire les deux. De plus, ISAKMP a été conçu pour être extensible à la gestion de clés de diffusion groupée à la fois pour la diffusion groupée IP et pour la sécurité de la diffusion groupée de couche application [RFC2408]. Donc, les protocoles de gestion de clés de diffusion groupé peuvent utiliser les protocoles existants de phase 1 et 2 du ISAKMP standard, éventuellement avec les extensions nécessaires (comme GDOI [RFC3547] ou la sécurité de la diffusion groupée de couche application).

Ce service de sécurité décrit aussi la fonctionnalité de la communication relative à la gestion de clé parmi différents serveurs GCKS dans une conception de groupe réparti.

La gestion de clé de diffusion groupée apparaît dans les deux conceptions centralisée et répartie comme le montre la Figure 2 et est placée dans la zone Gestion de clés de groupe.

5.6 Gestion de la politique de diffusion groupée

Ce service de sécurité traite toutes les questions qui se rapportent à la politique de groupe de diffusion groupée incluant la politique d'adhésion et la politique de gestion des clés de diffusion groupée. Bien sûr, une des premières tâches en précisant la définition de ce service de sécurité est d'identifier les différentes zones de politique de diffusion groupée. La gestion de la politique de diffusion groupée inclut la conception du serveur de politique pour la sécurité de la diffusion groupée, la définition des politiques particulières qui vont être utilisées pour la diffusion groupée IP et la sécurité de la diffusion groupée de couche application, et les protocoles de communication entre le serveur de politique et le serveur de clés. Ce service de sécurité peut être réalisé en utilisant une infrastructure de politique standard comme une architecture de point de décision de politique (PDP, *Policy Decision Point*) et de point d'application de politique (PEP, *Policy Enforcement Point*) [RFC2748]. Donc, il peut n'être pas nécessaire de réinventer une nouvelle architecture pour la politique de sécurité de la diffusion groupée. Au minimum, cependant, ce service de sécurité sera réalisé dans un ensemble de définitions de politique, comme des conditions et actions de sécurité de la diffusion groupée.

Le service de sécurité Gestion de la politique de diffusion groupée décrit la fonction de communication entre une instance d'un GCKS et une instance de serveur de politique. Les informations transmises peuvent inclure des politiques concernant les groupes, les membres, la définition du matériel de chiffrement et leurs utilisations permisses, et d'autres informations. Ce service de sécurité décrit aussi la communication entre les serveurs de politique. Le membres du groupe ne sont pas supposés participer directement à ce service de sécurité. Cependant, cette option n'est pas exclue.

6. Considérations pour la sécurité

Le présent document décrit un cadre architectural pour protéger le trafic de diffusion groupée et de groupe par des protocoles de chiffrement. Trois zones fonctionnelles sont identifiées au sein du cadre de référence. Chaque zone fonctionnelle a ses propres considérations de sécurité, et elles sont exposées ci-dessous.

Ce cadre architectural est de bout en bout, et ne s'appuie pas sur le réseau qui connecte les contrôleurs de groupe et les membres du groupe. Il ne tente pas non plus de résoudre les questions de sécurité dans les infrastructures d'acheminement en envoi individuel ou en diffusion groupée, ni dans les protocoles de contrôle d'admission de diffusion groupée. Les attaques de déni de service, de suppression de message, et autres attaques actives contre les infrastructures d'acheminement en envoi individuel ou en diffusion groupée ne sont pas en tant que telles visées par ce cadre. Le paragraphe 1.1 décrit les relations de l'infrastructure réseau avec l'architecture de sécurité de groupe de diffusion groupée.

6.1 Traitement des données de diffusion groupée

Les protocoles cryptographiques qui protègent les données de diffusion groupée sont chargés d'assurer la confidentialité et l'authentification du groupe. Ils devraient aussi être capables d'assurer l'authentification de la source pour identifier de façon univoque les envoyeurs au groupe. La protection des données de diffusion groupée contre la répétition est aussi désirable, mais n'est pas toujours possible. Ceci est dû à la complexité de la maintenance de l'état de protection contre la répétition pour de multiples envoyeurs. Le paragraphe 3.1 précise les exigences de sécurité pour cette zone.

6.2 Gestion de la clé de groupe

Les protocoles de gestion de clé de groupe fournissent les clés de chiffrement et la politique aux membres des groupes. Ils sont

chargés d'authentifier et d'autoriser les membres du groupe avant de leur révéler les clés, et d'assurer la confidentialité et l'authentification de ces clés durant le transit. Ils sont aussi chargés de fournir les moyens de changer les clés du groupe, lorsque la politique spécifie une durée de vie pour les clés. Ils sont aussi chargés de la révocation des adhésions au groupe, une fois qu'un ou plusieurs membres du groupe ont eu leur autorisation d'être membre du groupe révoquée. Le paragraphe 3.2 décrit plus en détails les exigences de sécurité de cette zone.

6.3 Politiques de sécurité de diffusion groupée

Les protocoles cryptographiques qui fournissent les politiques de sécurité de la diffusion groupée sont chargés de distribuer cette politique afin que l'intégrité de la politique soit maintenue. Si la politique elle même est confidentielle, ils sont aussi chargés d'authentifier les contrôleurs de groupe et les membres des groupes, et d'assurer la confidentialité de la politique durant le transit.

7. Remerciements

Beaucoup du texte du présent document découle de deux articles de recherches. La cadre pour le présent document vient d'un article co-rédigé par Thomas Hardjono, Ran Canetti, Mark Baugher, et Pete Dinsmore. La description de la GSA vient d'un document co-rédigé par Hugh Harney, Mark Baugher, et Thomas Hardjono. George Gross a suggéré un certain nombre d'améliorations qui ont été incluses dans les versions finales du présent document.

8. Références

8.1 Références normatives

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

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Association de sécurité Internet et protocole de gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

8.2 Références pour information

[BMS] D. Balenson, D. McGrew, A. Sherman, "Key Management for Large Dynamic Groups: One-Way Function Trees and Amortized Initialization", http://www.securemulticast.org/draft-balenson-groupkeymgmt-oft-00.txt, Travail en cours, février 1999.

[BCCR] M. Baugher, R. Canetti, P. Cheng, P. Rohatgi, "MESP: A Multicast Framework for the IPsec ESP", Travail en cours, octobre 2002.

[CCPRRS] Canetti, R., Cheng P. C., Pendarakis D., Rao, J., Rohatgi P., Saha D., "An IPSec-based Host Architecture for Secure Internet Multicast", http://www.isoc.org/isoc/conferences/ndss/2000/proceedings/028.pdf, NDSS 2000.

[Din] Dinsmore, P., Balenson, D., Heyman, M., Kruus, P., Scace, C., and Sherman, A., "Policy-Based Security Management for Large Dynamic Groups: An Overview of the DCCM Project", DARPA Information Survivability Conference and Exposition, http://download.nai.com/products/media/nai/doc/discex-110199.doc.

[McD] McDaniel, P., Honeyman, P., and Prakash, A., "Antigone: A Flexible Framework for Secure Group Communication", Proceedings of the Eight USENIX Security Symposium, pp 99-113, août 1999.

[RFC2093] H. Harney, C. Muckenhirn, "Spécification du protocole de gestion de clé de groupe (GKMP)", juillet 1997. *(Exp)*

[RFC2094] H. Harney, C. Muckenhirn, "Architecture du protocole de gestion de clé de groupe (GKMP)", juillet 1997. *(Exp.)*

[RFC2362] D. Estrin et autres, "Mode épars de diffusion groupée indépendante du protocole (PIM-SM) : Spécification du protocole", juin 1998. *(Obsolète, voir* RFC4601, *RFC5059*)

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

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

[RFC2627] D. Wallner, E. Harder, R. Agee,"Gestion de clés en diffusion groupé : problèmes et architectures", juin 1999. *(Info.)*

[RFC2663] P. Srisuresh, M. Holdrege, "Terminologie et considérations sur les traducteurs d'adresse réseau IP (NAT)", août 1999. *(Information)*

[RFC2748] D. Durham et autres, "Protocole COPS (Service commun de politique ouverte)", janvier 2000. (*MàJ par* RFC4261) *(P.S.)*

[RFC3019] B. Haberman, R. Worzella, "Base de données d'informations de gestion IP version 6 pour le protocole de découverte d'écoutant de diffusion groupée", janvier 2001. *(P.S.)*

[RFC3376] B. Cain et autres, "Protocole Internet de gestion de groupe, IGMP version 3", octobre 2002. *(P.S.)*

[RFC3453] M. Luby et autres, "Utilisation de la correction d'erreur directe (FEC) en diffusion groupée fiable", décembre 2002. *(Info.)*

[RFC3547] M. Baugher, B. Weis, T. Hardjono et H. Harney, "Le domaine d'interprétation de groupe", juillet 2003. *(Obsolète, voir la* RFC6407)

[RFC3830] J. Arkko et autres, "MIKEY : Gestion de clé multimédia pour l'Internet", août 2004. (*MàJ par* RFC4738) *(P.S.)*

[RFC4046] M. Baugher et autres, "Architecture de gestion de clé de groupe de diffusion groupée sécurisée (MSEC)", avril 2005. *(Info.)*

[RFC4082] A. Perrig et autres, "Authentification de flux tolérante aux pertes en temps efficace (TESLA) : Introduction à la transformation d'authentification de source de diffusion groupée", juin 2005.

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*

[RFC4535] H. Harney et autres, "GSAKMP : protocole de gestion de clés d'association de groupe sécurisé", juin 2006. *(P.S.)*

[STW] M., Steiner, Tsudik, G., Waidner, M., "CLIQUES: A New Approach to Group key Agreement", IEEE ICDCS'98 , mai 1998.

9. Adresse des auteurs

Thomas Hardjono
VeriSign
487 E. Middlefield Rd.
Mountain View, CA 94043
USA
téléphone : (650) 426-3204
mél : thardjono@verisign.com

Brian Weis
Cisco Systems
170 W. Tasman Drive,
San Jose, CA 95134-1706
USA
téléphone : (408) 526-4796
mél : bew@cisco.com

10. Déclaration complète de droits de reproduction

Propriété intellectuelle

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