Groupe de travail RéseauM. Baugher, Cisco
Request for Comments : 4046
Catégorie : Information
Traduction Claude Brière de L'Isle

M. Baugher, Cisco
R. Canetti, IBM
L. Dondeti, Qualcomm
F. Lindholm, Ericsson
avril 2005

Architecture de gestion de clé de groupe de sécurité de diffusion groupée (MSEC)

Statut du présent 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 l'architecture commune pour que les protocoles de gestion de clé de sécurité de diffusion groupée (MSEC, *Multicast Security*) prennent en charge divers protocoles de sécurité de couche application, transport, et réseau. Il définit aussi l'association de sécurité de groupe (GSA, *group security association*) et décrit les protocoles de gestion de clé qui aident à établir une GSA. Le cadre et les lignes directrices décrits dans le présent document permettent une conception modulaire et souple des protocoles de gestion de clé de groupe pour différents réglages qui sont particuliers aux besoins des applications. Les protocoles de gestion de clé MSEC peuvent être utilisés pour faciliter les communications sûres de un à plusieurs, de plusieurs à plusieurs, ou de un à un.

Table des matières

1. Introduction : objet du présent document

Le présent document définit une architecture commune pour que les protocoles de gestion de clé de sécurité de diffusion groupée (MSEC, *Multicast Security*) prennent en charge divers protocoles de sécurité de couche application, transport, et réseau. Il définit aussi l'association de sécurité de groupe (GSA, *group security association*) et décrit les protocoles de gestion de clé qui aident à établir une GSA. Le cadre et les lignes directrices décrits dans le présent document permettent une conception modulaire et souple des protocoles de gestion de clé de groupe pour différents réglages qui sont particuliers aux besoins des applications. Les protocoles de gestion de clé MSEC peuvent être utilisés pour faciliter les communications sûres de un à plusieurs, de plusieurs à plusieurs, ou de un à un.

Les applications de groupe et de diffusion groupée ont dans les réseaux IP des exigences de sécurité diverses [TAXONOMY]. Leurs exigences de gestion de clé, reprises brièvement au paragraphe 2.0, incluent la prise en charge des protocoles de sécurité de couche inter réseau, transport, et application. Certaines applications réalisent un fonctionnement plus simple en faisant fonctionner les messages de gestion de clé sur un canal sûr pré établi (par exemple, TLS ou IPsec). D'autres protocoles de sécurité bénéficient d'un protocole de gestion de clé qui peut fonctionner sur un protocole déjà déployé d'initialisation ou de gestion de session (par exemple, SIP ou RTSP). Finalement, certains bénéficient d'un protocole de gestion de clé léger qui n'exige que peu d'allers-retours. Pour toutes ces raisons, les protocoles de sécurité des données de couche application, transport, et IP (par exemple, SRTP [RFC3711] et IPsec [RFC2401]) bénéficient des différents systèmes de gestion de clé de groupe. Le présent document définit une architecture et une conception communes pour tous les protocoles de gestion de clé de groupe (GKM, *Group Key Management*).

Cette architecture commune pour la gestion de clé de groupe est appelée l'architecture de gestion de clé de groupe MSEC. Elle se fonde sur le modèle de contrôle de groupe ou de serveur de clé développé dans GKMP [RFC2094] et assumés par les algorithmes de gestion de clé de groupe comme LKH [RFC2627], OFT [OFT], et MARKS [MARKS]. Il y a d'autres approches qui ne sont pas prises en compte dans cette architecture, comme le protocole de gestion de clé de groupe très répartie Cliques [CLIQUES] ou les schémas de gestion de clé en diffusion [FN93], [Wool]. La gestion de clé MSEC peut en fait être complémentaire des autres concepts de gestion de clé de groupe, mais l'intégration de la gestion de clé de groupe MSEC avec Cliques, la gestion de clé en diffusion, ou autres systèmes de clé de groupe n'est pas examinée dans le présent document.

Les protocoles de gestion de clé sont difficiles à concevoir et valider. L'architecture commune décrite dans le présent document facilite cette tâche en définissant des abstractions communes et un concept global qui peut être spécialisé pour des utilisations différentes.

Le présent document s'appuie sur le document du groupe de recherche SmuG de l'IRTF sur les blocs de construction de la gestion de clé de groupe [GKMBB] et l'étend, et fait partie du document de feuille de route MSEC. L'architecture de MSEC [RFC3740] définit une architecture complète de sécurité de diffusion groupée ou de groupe, dont la gestion de clé est une composante.

Le reste de ce document est organisé comme suit. La Section 2 discute de la sécurité, des exigences de performances et d'architecture pour un protocole de gestion de clé de groupe. La Section 3 présente les principes globaux de la conception architecturale. La Section 4 décrit en détails le protocole d'enregistrement, et la Section 5 fait de même pour le protocole de changement de clé. La Section 6 considère l'interface avec l'association de sécurité de groupe (GSA, *Group Security Association*). La Section 7 passe en revue les questions d'adaptabilité pour les protocoles de gestion de clé de groupe et la Section 8 discute les considérations sur la sécurité.

2. Exigence d'un protocole de gestion de clé de groupe

Un protocole de gestion de clé de groupe (GKM) prend en charge la communication protégée entre membres d'un groupe sécurisé. Un groupe sécurisé est une collection de principaux, appelés membres, qui peuvent être des envoyeurs, des receveurs, ou à la fois des receveurs et des envoyeurs aux autres membres du groupe. L'appartenance au groupe peut varier dans le temps. Un protocole de gestion de clé de groupe aide à assurer que seuls les membres d'un groupe sécurisé peuvent obtenir l'accès aux données du groupe (en obtenant l'accès aux clés du groupe) et peuvent authentifier les données du groupe. Le but d'un protocole de gestion de clé de groupe est de fournir aux membres légitimes du groupe l'état de chiffrement à jour dont ils ont besoin pour assurer le secret et l'authentification.

Les applications de diffusion groupée, comme la diffusion vidéo et le transfert de fichier en diffusion groupée, ont normalement les exigences de gestion de clé suivantes (voir aussi [TAXONOMY]). Noter que cette liste n'est ni exhaustive

ni applicable à toutes les applications.

1. Les membres du groupe reçoivent des associations de sécurité qui incluent des clés de chiffrement, des clés d'authentification/intégrité, une politique cryptographique qui décrit les clés, et des attributs comme un indice pour référencer l'association de sécurité (SA) ou des objets particuliers contenus dans la SA.

2. En plus de la politique associée aux clés de groupes, le propriétaire du groupe ou le contrôleur de groupe et serveur de clés (GCKS, *Group Controller and Key Server*) peut définir et appliquer l'adhésion au groupe, la gestion de clé, la sécurité des données, et d'autres politiques qui peuvent ou non être communiqués à tous les membres.

3. Les clés ont une durée de vie pré déterminée et peuvent être rafraîchies périodiquement.

4. Le matériel de chiffrement devrait être livré de façon sécurisée aux membres du groupe afin qu'il soit secret, protégé en intégrité et vérifiable et obtenu d'une source autorisée.

5. Le protocole de gestion de clé devrait être sécurisé contre les attaques en répétition et de déni de service (DoS) (voir la Section des considérations sur la sécurité).

6. Le protocole devrait faciliter l'ajout et la suppression des membres du groupe. Les membres qui sont ajoutés peuvent facultativement être privés d'accès au matériel de chiffrement utilisé avant qu'ils se joignent au groupe, et les membres supprimés devraient perdre l'accès au matériel de chiffrement à la suite de leur départ.

7. Le protocole devrait prendre en charge une opération adaptable de changement des clés du groupe sans échanges en envoi individuel entre les membres et un contrôleur de groupe et serveur de clés (GCKS) pour éviter de submerger un GCKS qui gère un grand groupe.

8. Le protocole devrait être compatible avec l'infrastructure et les besoins de performances de l'application de sécurité des données, comme les protocoles de sécurité IPsec AH et ESP, et/ou les protocoles de sécurité de couche d'application comme SRTP [RFC3711].

9. Le protocole de gestion de clé devrait offrir un cadre pour remplacer ou renouveler les transformations, l'infrastructure d'autorisation, et les systèmes d'authentification.

10. Le protocole de gestion de clé devrait être sécurisé contre la collusion entre les membres exclus et des non membres. Spécifiquement, la collusion ne doit pas résulter en ce que des attaquants obtiennent des secrets de groupe supplémentaires dont chacun est individuellement privé. En d'autres termes, combiner les connaissances d'entités qui se coalisent ne doit pas résulter en la révélation de secrets supplémentaires du groupe.

11. Le protocole de gestion de clé devrait fournir un mécanisme pour récupérer en toute sécurité de la compromission de tout ou partie du matériel de chiffrement.

12. Le protocole de gestion de clé peut avoir besoin de traiter des problèmes de déploiement dans le monde réel comme la traversée de NAT et l'interface avec les mécanismes d'authentification traditionnels.

À la différence des protocoles normaux de négociation de clé et de SA en envoi individuel comme TLS et IKE, les protocoles de gestion de clé de groupe en diffusion groupée fournissent une capacité de téléchargement de SA et de clé. Cette caractéristique peut être utile pour la communication en point à point aussi bien qu'en diffusion groupée, de sorte qu'un protocole de gestion de clé de groupe peut être utile pour des applications d'envoi individuel. Les protocoles de gestion de clé de groupe peuvent être utilisés pour protéger des communications en diffusion groupée ou en envoi individuel entre les membres d'un groupe sécurisé. Une communication de sous groupe sécurisé est aussi possible en utilisant la SA de groupe.

Il y a d'autres exigences pour le fonctionnement d'un petit groupe dont tous les membres sont des envoyeurs potentiels. Dans ce cas, le temps d'établissement du groupe peut devoir être optimisé pour prendre en charge un environnement de petit groupe très interactif [RFC2627].

L'architecture de gestion de clé actuelle couvre la communication sécurisée dans de grands groupes à un seul envoyeur, comme des groupes de diffusion groupée spécifiques d'une source. Le fonctionnement adaptable à une gamme de tailles de groupe est aussi une caractéristique désirable, et un meilleur protocole de gestion de clé de groupe va prendre en charge des groupes à un seul envoyeur aussi bien que des groupes qui ont de nombreux envoyeurs. Il se peut qu'aucun protocole de gestion de clé ne puisse pas satisfaire seul les exigences d'adaptabilité de toutes les applications de sécurité de groupe.

Il est utile de développer deux non exigences : les mesures de protection techniques [TPM] et la gestion de clé diffusée. Les mesures de protection techniques sont utilisées pour des choses comme la protection contre la copie en empêchant l'appareil utilisateur d'avoir un accès aisé aux clés de groupe. Il n'y a pas de raison qu'un protocole de gestion de clé de groupe ne puisse pas être utilisé dans un environnement où les clés sont conservées dans une mémorisation à l'épreuve de l'altération, en utilisant divers types de matériels ou logiciels pour mettre en œuvre les mesures de protection techniques. Pour rester cependant simple, l'architecture MSEC de gestion de clé décrite dans le présent document ne traite pas de la conception des la protection technique.

La seconde non exigence est la gestion de clé en diffusion quand il n'y a pas de canal de retour [FN93], [JKKV94] ou pour un appareil qui n'est pas en réseau comme un lecteur de vidéodisque numérique. On suppose le fonctionnement du réseau IP avec une communication bidirectionnelle, mais asymétrique, et des procédures d'échange de clé authentifié qui peuvent être utilisées pour l'enregistrement des membres. Les applications de diffusion peuvent utiliser un message unidirectionnel de protocole de gestion de clé de groupe Internet et un message unidirectionnel de changement de clé, comme décrit ci-dessous.

3. Conception globale de l'architecture de gestion de clé de groupe

L'architecture globale de gestion de clé de groupe se fonde sur un modèle de contrôleur de groupe [RFC2093], [RFC2094], [RFC2627], [OFT], [RFC4535], [RFC3547] avec un seul propriétaire du groupe comme racine de confiance. Le propriétaire du groupe désigne un contrôleur de groupe pour l'enregistrement des membres et le changement de clé de GSA.

3.1 Vue d'ensemble

Le but principal d'un protocole de gestion de clé de groupe est de fournir en toute sécurité aux membres du groupe une association de sécurité (SA) à jour, qui contient les informations nécessaires pour sécuriser les communications du groupe (c'est-à-dire, les données du groupe). On appelle cette SA la SA de données. Pour atteindre ce but, l'architecture de gestion de clé de groupe définit les protocoles suivants .

(1) Protocole d'enregistrement
C'est un protocole d'envoi individuel entre le contrôleur de groupe/serveur de clés (GCKS) et un membre postulant du groupe. Dans ce protocole, le GCKS et le membre postulant s'authentifient mutuellement. Si l'authentification réussit et si le GCKS trouve que le membre postulant est autorisé, il fournit alors au membre postulant les informations suivantes :
(a) Des informations suffisantes pour initier la SA de données chez le membre postulant. Ces informations ne sont données que si la politique de sécurité du groupe invite à initialiser la SA de données au moment de l'enregistrement, au lieu de ou en plus de, au titre du protocole de changement de clé.
(b) Des informations suffisantes pour initier une SA de changement de clé chez le membre postulant (voir les détails de cette SA ci-dessous). Ces informations sont données si la politique de sécurité du groupe invite à un protocole de changement de clé. Le protocole d'enregistrement doit assurer que le transfert des informations du GCKS au membre est d'une manière authentifiée et confidentielle sur une association de sécurité. On appelle cette SA la SA d'enregistrement. Un protocole de désenregistrement complémentaire sert à supprimer explicitement l'état de la SA d'enregistrement. Les membres peuvent choisir de supprimer l'état de SA d'enregistrement.

(2) Protocole de changement de clé
Un GCKS peut périodiquement mettre à jour ou changer la SA de données, en envoyant des informations de changement de clés aux membres du groupe. Les messages de changement de clé peuvent résulter de changements des membres du groupe, de changements de la politique de sécurité du groupe, de la création de nouvelles clés de protection du trafic (TPK, *traffic protection key*) (voir au paragraphe suivant) pour le groupe particulier, ou de l'expiration de la clé. Les messages de changement de clé sont protégés par la SA de changement de clé, qui est initialisée dans le protocole d'enregistrement. Ils contiennent des informations pour mettre à jour la SA de changement de clé et/ou la SA de données et peuvent être envoyés par diffusion groupée aux membres du groupe ou par envoi individuel du GCKS à un membre du groupe particulier.

Noter qu'il y a d'autres moyens pour gérer la SA de données (par exemple, l'expiration ou le rafraîchissement) sans interaction entre le GCKS et les membres. Par exemple dans [MARKS], le GCKS pré détermine les TPK pour les différentes périodes de la durée de vie du groupe sécurisé et distribue les clés aux membres sur la base de leurs périodes d'adhésion. D'autres schémas comme la dissolution par le GCKS du groupe sécurisé et le lancement d'un nouveau groupe avec une nouvelle SA de données sont aussi possibles, bien que ce soit normalement limité aux petits groupes.

Les messages de changement de clé sont authentifiés en utilisant une des deux options suivantes :

(1) Utiliser l'authentification de la source [TAXONOMY], c'est-à-dire, permettre à chaque membre du groupe de vérifier qu'un message de changement de clé a bien pour origine le GCKS et personne d'autre.

(2) Utiliser seulement une authentification fondée sur le groupe avec une clé symétrique. Les membres peuvent seulement être assurés que les messages de changement de clé ont leur origine dans le groupe. Donc, ceci n'est applicable que quand tous les membres du groupe sont estimés ne pas se faire passer pour le GCKS. L'authentification de groupe pour les messages de changement de clés est normalement utilisée quand le chiffrement à clé publique ne convient pas pour ce groupe.

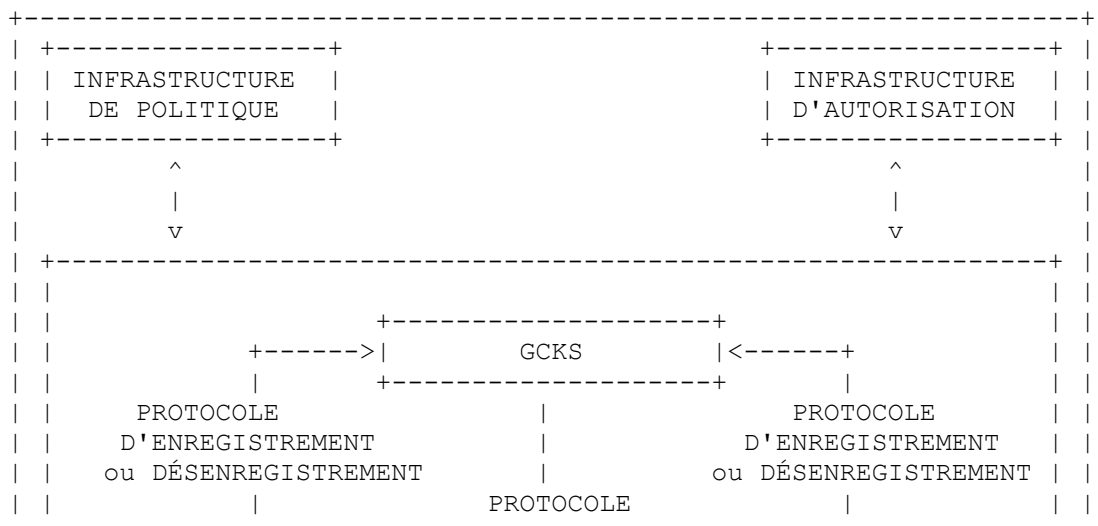
Le protocole de changement de clé assure que tous les membres reçoivent en temps utile les informations de changement de clé. De plus, le protocole de changement de clé spécifie des mécanismes pour que les parties contactent le GCKS et se resynchronisent si leurs clés sont arrivées à expiration et que des clés à jour n'ont pas encore été reçues. Le protocole de changement de clé pour des groupes de grande taille offre des mécanismes pour éviter des problèmes d'implosion et pour assurer la fiabilité de la livraison du matériel de chiffrement.

Bien que la SA de changement de clé soit établie par le protocole d'enregistrement, elle est mise à jour en utilisant un protocole de changement de clé. Quand un membre quitte le groupe, il détruit sa copie locale de la GSA. Utiliser un message de désenregistrement peut être un moyen efficace pour qu'un membre informe le GCKS qu'il a détruit, ou est sur le point de détruire, les SA. Un tel message peut inviter le GCKS à supprimer cryptographiquement le membre du groupe (c'est-à-dire, d'empêcher le membre d'avoir accès aux futures communications du groupe). Cependant, dans les applications de diffusion groupée à grande échelle, le désenregistrement peut causer une implosion au GCKS.

3.2 Description détaillée de l'architecture GKM

La Figure 1 décrit la conception générale d'un protocole de GKM. Chaque membre du groupe, envoyeur ou receveur, utilise le protocole d'enregistrement pour obtenir un accès autorisé et authentifié à un groupe particulier, ses politiques, et ses clés. Les deux types de clés de groupe sont les clés de chiffrement de clé (KEK, *key encryption key*) et les clés de chiffrement de trafic (TEK, *traffic encryption key*). Pour l'authentification des messages ou données de changement de clés du groupe, des clés d'intégrité de clé ou d'intégrité du trafic peuvent aussi être utilisées. On utilise le terme de clés de protection pour se référer aux clés d'intégrité et aux clés de chiffrement. Par exemple, le terme de clés de protection du trafic (TPK, *traffic protection key*) est utilisé pour noter la combinaison d'une TEK et d'une clé d'intégrité du trafic, ou le matériel de chiffrement utilisé pour les générer.

La KEK peut être une seule clé qui protège le message de changement de clé, qui contient normalement une nouvelle SA de changement de clé (contenant une KEK) et/ou une SA de données (contenant une TPK/TEK). Une SA de changement de clé peut aussi contenir un vecteur de clés qui fait partie d'un algorithme d'adhésion de clé de groupe [RFC2627], [OFT], [TAXONOMY], [SD1], [SD2]. Le protocole de sécurité des données utilise les TPK pour protéger les flux, les fichiers, ou autres données envoyées et reçues par le protocole de sécurité des données. Donc, le protocole d'enregistrement et/ou le protocole de changement de clé établit la ou les KEK et/ou les TPK.



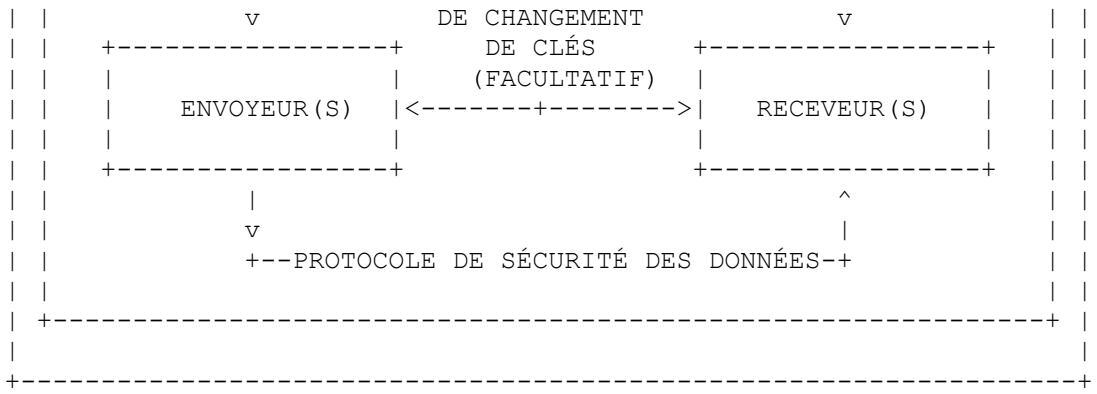


Figure 1 : Modèle d'association de sécurité de groupe

Un échange de protocole d'enregistrement réussi donne plusieurs résultats distincts :

- Si le GCKS utilise des messages de changement de clé, le membre admis reçoit la SA de changement de clé. Celle-ci contient la politique de changement de clé du groupe (noter qu'il n'est pas nécessaire de révéler toute la politique aux membres) et au moins une KEK de groupe. De plus, le GCKS envoie une clé d'intégrité de clé de groupe pour la protection de l'intégrité des messages de changement de clé. Si un algorithme de gestion de clé de groupe est utilisé pour un changement de clé efficace, le GCKS envoie aussi une ou plusieurs KEK comme spécifié par la politique de distribution de clé de l'algorithme de gestion de clé de groupe.

- Si des messages de changement de clé ne sont pas utilisés pour le groupe, le membre admis reçoit des TPK (au titre des SA de sécurité des données) qui sont passées au protocole de sécurité des données du membre (comme IKE le fait pour IPsec).

- Le GCKS peut passer une ou plusieurs TPK au membre même si les messages de changement de clé sont utilisés, pour des raisons d'efficacité et conformément à la politique du groupe.

Le GCKS crée la KEK et les TPK et les télécharge à chaque membre, car la KEK et les TPK sont communes au groupe entier. Le GCKS est une entité logique séparée qui effectue l'authentification et l'autorisation des membres en accord avec la politique du groupe qui est établi par le propriétaire du groupe. Le GCKS peut présenter un accréditif signé par le propriétaire du groupe au membre du groupe, de sorte que ce membre peut vérifier l'autorisation du GCKS. Le GCKS, qui peut être colocalisé avec un membre ou être physiquement séparé, fait fonctionner le protocole de changement de clé pour pousser les messages de changement de clé qui contiennent les KEK rafraîchies, les nouvelles TPK, et/ou des TPK rafraîchies aux membres. Noter que certains algorithmes de gestion de clé de groupe rafraîchissent toutes les KEK (potentiellement) tandis que d'autres ne rafraîchissent que la KEK de groupe.

Autrement, l'envoyeur peut transmettre les messages de changement de clé au nom du GCKS quand il utilise un mécanisme d'accréditif qui prend en charge la délégation. Donc, il est possible à l'envoyeur, ou aux autres membres, de générer du matériel de chiffrement (des TPK chiffrées dans la KEK de groupe) lorsque il génère des données en diffusion groupée ou en envoi individuel. Comme mentionné ci-dessus, le message de changement de clé peut être envoyé en utilisant une livraison en envoi individuel ou en diffusion groupée. À réception d'une TPK (au titre d'une SA de données) via un message de changement de clé ou un échange de protocole d'enregistrement, le bloc fonctionnel de gestion de clé de groupe du membre va fournir l'association de sécurité (SA) nouvelle ou mise à jour au protocole de sécurité des données. Cela protège cles données envoyées de l'envoyeur au receveur.

Les SA de données protègent les données envoyées sur l'arc étiqueté PROTOCOLE DE SÉCURITÉ DES DONNÉES montré à la Figure 1. Une seconde SA, la SA de changement de clés, est facultativement établie par le protocole de gestion de clé pour les messages de changement de clé comme montré à la Figure 1 par l'arc étiqueté PROTOCOLE DE CHANGEMENT DE CLÉ. Le message de changement de clé est facultatif parce que toutes les clés, KEK et TPK, peuvent être livrées par les échanges du protocole d'enregistrement montré à la Figure 1, et ces clés peuvent n'avoir pas besoin d'être mises à jour. Le protocole d'enregistrement est protégé par une troisième SA, en envoi individuel, la SA entre le GCKS et chaque membre. Elle est appelée la SA d'enregistrement. Il se peut qu'il ne soit pas besoin que la SA d'enregistrement reste en place après l'achèvement des échanges du protocole d'enregistrement. Le protocole de désenregistrement peut être utilisé quand est souhaité une suppression explicite de la SA (comme quand se termine un appel téléphonique ou une conférence). Les trois SA composent la GSA. La seule SA facultative est la SA de changement de clés.

La Figure 1 montre deux blocs qui sont externes au protocole de gestion de clé de groupe : les infrastructures de politique et d'autorisation sont discutées au paragraphe 6.1. Le document d'architecture de sécurité de diffusion groupée précise les SA et leur utilisation au titre de l'architecture complète d'une solution de sécurité de diffusion groupée [RFC3740].

3.3 Propriétés du concept

Le concept du paragraphe 3.2 réalise un fonctionnement adaptable en (1) permettant le découplage de l'échange de clés authentifiées dans un protocole d'enregistrement d'un protocole de changement de clé, (2) permettant que le protocole de changement de clé utilise la poussée en envoi individuel ou la distribution en diffusion groupée des clés de groupe et de données comme option, (3) permettant que toutes les clés soient obtenues par le protocole d'enregistrement en envoi individuel, et (4) délégant la fonction de GCKS parmi plusieurs entités, c'est-à-dire, en permettant un fonctionnement réparti du GCKS.

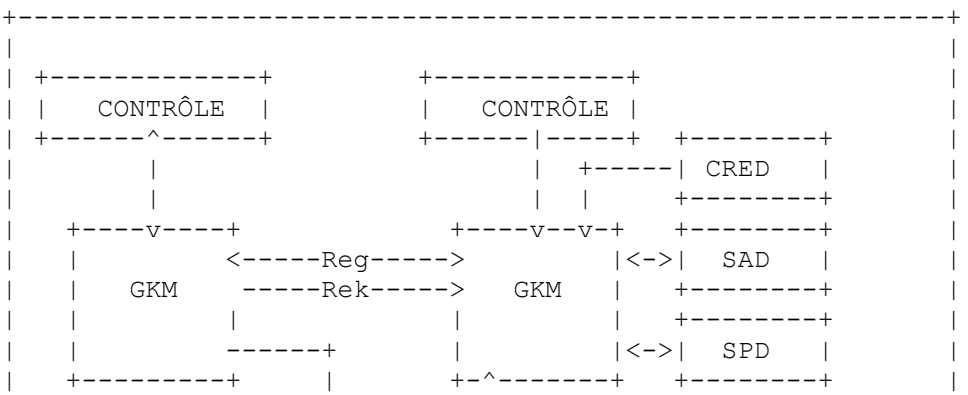
Un fonctionnement de haute capacité est obtenu en (1) amortissant les coûts élevés de calcul de chiffrement asymétrique sur plusieurs clés de données utilisées par les protocoles de sécurité des données, (2) prenant en charge la distribution en diffusion groupée des clés symétriques de groupe et de données, et (3) prenant en charge des algorithmes de révocation comme LKH [RFC2627], [OFT], [SD1], [SD2] qui permettent aux membres d'être ajoutés ou supprimés à une complexité d'espace/temps logarithmique plutôt linéaire. Le protocole d'enregistrement peut utiliser un chiffrement asymétrique pour authentifier les membres arrivants et facultativement d'établir la KEK de groupe. Un chiffrement asymétrique tel que l'accord de clé Diffie-Hellman et/ou des signatures numériques est amorti sur la durée de vie de la KEK de groupe. Une SA de données peut être établie sans utiliser de chiffrement asymétrique ; les TPK sont simplement chiffrées dans la KEK symétrique et envoyées en envoi individuel ou en diffusion groupée dans le protocole de changement de clé.

Le dessin des protocoles d'enregistrement et de changement de clé est souple. Le protocole d'enregistrement établit une SA de changement de clés ou une ou plusieurs SA de données ou les deux types de SA. Au moins une des SA est présente (autrement, la SA d'enregistrement n'a pas d'objet). La SA de changement de clés peut mettre à jour la SA de changement de clés, ou établir ou mettre à jour une ou plusieurs SA de données. Les protocoles ou configurations individuels peuvent utiliser cette souplesse pour obtenir un fonctionnement efficace.

3.4 Diagramme de blocs de gestion de clé de groupe

Dans le diagramme de blocs de la Figure 2, les protocoles de gestion de clé de groupe fonctionnent entre un GCKS et le membre principal pour établir une association de sécurité de groupe (GSA). La GSA consiste en une SA de données, une SA de changement de clés facultative, et une SA d'enregistrement. Le GCKS peut utiliser un principal délégué, comme l'envoyeur, qui a des accréditifs de délégation signés par le GCKS. Le membre de la Figure 2 peut être un envoyeur ou un receveur de données en diffusion groupée ou en envoi individuel. Il y a deux blocs fonctionnels dans la Figure 2 qui sont marqués GKM, et il y a deux arcs entre eux qui décrivent les protocoles d'enregistrement de gestion de clé de groupe (reg) et de changement de clé (rek). Les échanges de message sont dans les protocoles d'établissement de GSA, qui sont le protocole d'enregistrement et le protocole de changement de clé décrits ci-dessus.

La Figure 2 montre qu'une spécification fonctionnelle complète de gestion de clé de groupe inclut beaucoup plus que l'échange de messages. Certains de ces blocs fonctionnels et les arcs entre eux sont particuliers d'un système d'exploitation (OS) ou d'un produit d'un fabricant, comme les spécifications de fabricants pour les produits qui prennent en charge des mises à jour aux bases de données d'associations de sécurité (SAD, *Security Association Database*) et aux bases de données de politique de sécurité (SPD, *Security Policy Database*) [RFC2367] IPsec. Divers fabricants définissent aussi les fonctions et interfaces des répertoires d'accréditifs, marqués CRED dans la Figure 2.



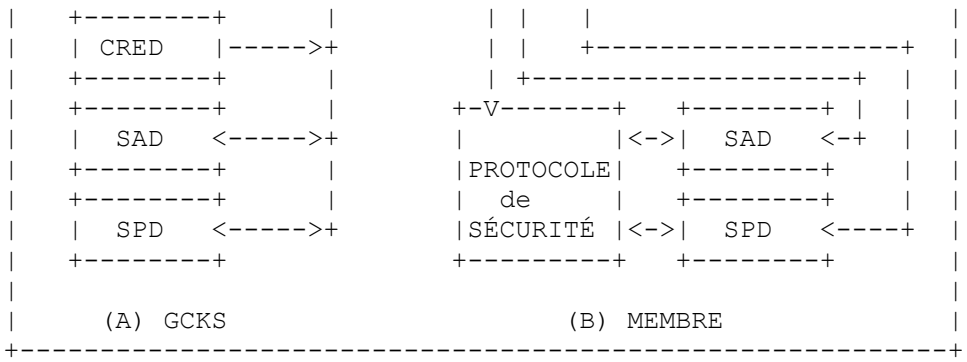


Figure 2 : Bloc de gestion de clé de groupe dans un hôte

La fonction CONTRÔLE indique au GCKS d'établir un groupe, d'admettre un membre, ou de supprimer un membre, ou elle indique à un membre de se joindre ou de quitter un groupe. CONTRÔLE inclut l'autorisation qui est soumise à la politique du groupe [GSPT] mais sa mise en œuvre est spécifique du GCKS. Pour des sessions de diffusion groupée à grande échelle, CONTRÔLE pourrait effectuer des fonctions d'annonce de session pour informer un membre potentiel du groupe qu'il peut se joindre au groupe ou recevoir les données du groupe (par exemple, un flux de transfert de fichiers protégé par un protocole de sécurité des données). Les annonces notifient aux membres du groupe d'établir des SA en diffusion groupée en avance de la transmission sûre des données en diffusion groupée. Le protocole de description de session (SDP, *Session Description Protocol*) est une des formes que peuvent prendre les annonces [RFC2327]. La fonction d'annonces peut être mise en œuvre dans un outil de répertoire de sessions, un guide de programme électronique (EPG, *electronic program guide*) ou par d'autres moyens. La fonction de sécurité des données ou d'annonces dirige la gestion de clé de groupe en utilisant une interface de programme d'application (API, *application programming interface*) qui est particulière à l'OS de l'hôte dans ce qu'il a de spécifique. Une API générique pour la gestion de clé de groupe est à l'étude, mais cette fonction est nécessaire pour permettre d'adapter l'établissement de la clé de groupe (KEK) et de données (TPK) à l'application particulière. Un programme d'application de GCKS va utiliser l'API pour initier les procédures d'établissement des SA au nom d'un protocole de sécurité dans lequel les membres se joignent aux groupes sécurisés et reçoivent les clés pour les flux, les fichiers, ou autres données.

Le but des échanges est d'établir une GSA par des mises à jour à la SAD d'une mise en œuvre de gestion de clé et d'un protocole de sécurité particulier. Le protocole de sécurité des données ("PROTOCOLE de SÉCURITÉ") de la Figure 2 peut s'étendre aux couches inter réseau et application ou fonctionner à la couche inter réseau, comme AH et ESP.

4. Protocole d'enregistrement

Le dessin du protocole d'enregistrement est souple et peut prendre en charge différents scénarios d'application. La solution de protocole d'enregistrement choisie reflète les exigences spécifiques des scénarios. En principe, il est possible de fonder un protocole d'enregistrement sur tout protocole de canal sûr, comme IPsec et TLS, ce qui est le cas dans GSAKMP tunnelé [tGSAKMP]. GDOI [RFC3547] réutilise IKE phase 1 comme canal sûr pour télécharger les SA de changement de clés et/ou de données. D'autres protocoles, comme MIKEY et GSAKMP, utilisent des échanges Diffie-Hellman authentifiés similaires à IKE phase 1, mais ils sont spécifiquement taillés pour que le téléchargement de clé réalise un fonctionnement efficace. On explique en détails la conception d'un protocole d'enregistrement dans le reste de cette Section.

4.1 Protocole d'enregistrement via portage ou réutilisation de protocole

Certains protocoles d'enregistrement ont besoin de tunneler à travers un protocole de signalisation des données pour tirer parti de la fonction de sécurité déjà existante, et/ou optimiser le temps d'établissement total de la session. Par exemple, un appel téléphonique a des limites de délai strictes pour le temps d'établissement. Il n'est pas possible d'avoir des échanges de sécurité en parallèle avec l'établissement de l'appel, car les échanges doivent souvent résoudre l'adresse. L'établissement de l'appel doit s'achever avant que l'appelant connaisse l'adresse de l'appelé. Dans ce cas, il peut être avantageux de tunneler les procédures d'échange de clé à l'intérieur de l'établissement d'appel [H.235], [RFC3830], afin que les deux puissent s'achever (ou échouer, voir ci-dessous) en même temps.

Le protocole d'enregistrement a des exigences différentes selon l'approche particulière de l'intégration/tunnelage. Ces exigences ne sont pas nécessairement des exigences de sécurité, mais vont avoir un impact sur la solution de sécurité

choisie. Par exemple, l'association de sécurité va certainement échouer si l'établissement d'appel échoue dans le cas de la téléphonie IP.

À l'inverse, le protocole d'enregistrement impose des exigences au protocole qui le tunnelle. Dans le cas de la téléphonie IP, l'établissement d'appel va généralement échouer quand l'établissement de l'association de sécurité échoue. Dans le cas de la vidéo à la demande, les protocoles comme RTSP qui portent les données de gestion de clé vont échouer quand une association de sécurité nécessaire ne peut pas être établie.

GDOI et MIKEY utilisent tous deux cette approche, mais d'une façon différente. MIKEY peut être tunnelé dans SIP et RTSP. Il tire parti des informations de session contenues dans ces protocoles et de la possibilité d'optimiser le temps d'établissement pour la procédure d'enregistrement. SIP exige qu'un protocole tunnelé utilise au plus un aller-retour (c'est-à-dire, deux messages). C'est aussi une exigence souhaitée de RTSP.

L'approche de GDOI tire parti de l'échange ISAKMP phase 1 déjà défini [RFC2409], et étend l'échange de phase 2 pour l'enregistrement. L'avantage est ici la réutilisation d'un protocole déployé avec succès et de la base de code, où l'échange de phase 2 défini est protégé par la SA créée par la phase 1. GDOI hérite aussi d'autres fonctions de ISAKMP, et est donc directement utilisable pour faire fonctionner les protocoles IPsec sur des services de diffusion groupée IP.

4.2 Propriétés des types d'échange d'enregistrement de remplacement

Les propriétés requises d'une conception de protocole d'enregistrement ont des compromis différents. Un protocole qui fournit le secret parfait vers l'avant et la protection de l'identité échange les performances ou l'efficacité contre une meilleure sécurité, tandis qu'un protocole qui se réalise en un ou deux messages peut sacrifier la fonction de sécurité (par exemple, la protection de l'identité) à l'efficacité.

La protection contre la répétition utilise généralement un horodatage ou un numéro de séquence. Le premier exige des horloges synchronisées, tandis que le second exige la conservation de l'état. Dans un protocole fondé sur l'horodatage, une antémémoire de répétition est nécessaire pour mémoriser les messages authentifiés (ou leurs hachages) reçus dans le biais d'horloge admissible. La taille de l'antémémoire de répétition dépend du nombre de messages authentifiés reçus durant le biais d'horloge admissible. Durant une attaque de DoS, l'antémémoire de répétition peut se trouver surchargée. Une solution est de surdimensionner l'antémémoire de répétition, mais cela peut conduire à une antémémoire de répétition trop grande. Une autre solution est de permettre que le biais d'horloge admissible soit changé de façon dynamique au démarrage. Durant une suspicion d'attaque de DoS, le biais d'horloge admissible est diminué afin que l'antémémoire de répétition devienne gérable.

Un mécanisme de défi/réponse (utilisant des noms occasionnels) diminue le besoin d'horloges synchronisées pour la protection contre la répétition quand l'échange utilise trois messages ou plus [MVV].

Des fonctions de sécurité supplémentaires deviennent possibles lorsque le nombre de messages admissibles dans le protocole d'enregistrement augmente. ISAKMP offre la protection de l'identité, par exemple, au titre d'un échange de six messages. Avec des caractéristiques de sécurité supplémentaires survient cependant une complexité accrue : la protection de l'identité, par exemple, exige non seulement des messages supplémentaires, mais peut résulter en des vulnérabilités à des attaques de DoS car l'authentification est effectuée à un stade tardif de l'échange après que des ressources ont déjà été allouées.

Dans tous les cas, il y a un compromis avec le nombre de message échangés, les services de sécurité désirés, et la quantité d'infrastructure nécessaire pour prendre en charge le service de gestion de clé de groupe. Alors que les protocoles qui utilisent deux ou même un message d'établissement ont une faible latence et exigences de calcul, ils peuvent exiger plus d'infrastructure comme une heure sécurisée ou offrent moins de sécurité comme l'absence de protection de l'identité. Ce qui est ou non un compromis acceptable dépend très largement de l'application et de son environnement.

4.3 Infrastructure pour les types d'échange d'enregistrement de remplacement

Le protocole d'enregistrement peut avoir besoin d'infrastructures externes pour traiter l'authentification et l'autorisation, la protection contre la répétition, l'intégrité conduite par le protocole, et éventuellement d'autres services de sécurité comme des horloges synchronisées de façon sûre. Par exemple, l'authentification et l'autorisation peuvent avoir besoin d'un déploiement de PKI (avec des certificats fondés sur l'autorisation ou une gestion séparée) ou peuvent être traités en utilisant une infrastructure d'AAA. La protection contre la répétition avec des horodatages exige une infrastructure ou protocole externe pour la synchronisation d'horloge.

Cependant, des infrastructures externes peuvent n'être pas toujours nécessaires ; par exemple des clés pré partagées sont utilisées pour l'authentification et l'autorisation. Ce peut être le cas si la base d'adhérents est relativement faible. Dans un scénario de conversation multimédia (par exemple, un appel VoIP entre deux personnes ou plus) ce peut être l'utilisateur final qui traite l'autorisation en acceptant/rejetant manuellement les appels entrants. Dans ce cas, la prise en charge d'une infrastructure peut n'être pas nécessaire.

4.4 Échange de désenregistrement

Le protocole d'établissement de session (par exemple, SIP, RTSP) qui transporte un échange d'enregistrement a souvent un protocole de désétablissement de session comme RTSP TEARDOWN [RFC2326] ou SIP BYE [RFC3261]. L'échange de désétablissement de session entre les points d'extrémité offre l'opportunité de signaler la fin de l'état de GSA aux points d'extrémité. Cet échange doit seulement être une notification unidirectionnelle par un des côtés que la GSA va être détruite. Pour l'authentification de cette notification, on peut utiliser une preuve de possession de la ou des clés de groupe par un côté ou l'autre. Certaines applications bénéficient d'un accusé de réception mutuel dans un échange à deux messages de signalisation de désétablissement de la GSA concomitant avec le désétablissement de la session, par exemple, session RTSP ou SIP. Dans ce cas, une preuve de possession bidirectionnelle peut servir pour un accusé de réception mutuel du désétablissement de la GSA.

5. Protocole de changement de clé

Le protocole de changement de clé de groupe est pour le transport des clés et des SA entre un GCKS et les membres d'un groupe de communications sécurisé. Le GCKS envoie des messages de changement de clé pour mettre à jour une SA de changement de clés, ou initialiser/mettre à jour une SA de données, ou les deux. Les messages de changement de clé sont protégés par une SA de changement de clés. Le GCKS peut mettre à jour la SA de changement de clés quand la composition du groupe change ou quand les KEK ou TPK arrivent à expiration. On se rappelle que les KEK correspondent à une SA de changement de clés et que les TPK correspondent à une SA de données.

Les propriétés suivantes sont souhaitables pour le protocole de changement de clé :
- o le protocole de changement de clé assure que tous les membres reçoivent les informations de changement de clé en temps utile,
- o le protocole de changement de clé spécifie les mécanismes qui permettent aux parties de contacter le GCKS et de se resynchroniser quand leurs clés arrivent à expiration et qu'aucune mise à jour n'a été reçue,
- o le protocole de changement de clé évite les problèmes d'implosion et assure la fiabilité de la livraison des informations de changement de clé.

On note de plus que le protocole de changement de clé est principalement chargé de l'adaptabilité de l'architecture de gestion de clé de groupe. Donc, il est impératif que les propriétés ci-dessus soient fournies de façon adaptable. Noter que des solutions existent dans la littérature (aussi bien des normes de l'IETF que des articles de recherche) pour des parties du problème. Par exemple, le protocole de changement de clé peut utiliser un algorithme adaptable de gestion de clé de groupe (GKMA, *Group Key Management Algorithm*) pour réduire le nombre de clés envoyées dans un message de changement de clé. Des exemples de GKMA sont LKH, OFT, des schémas fondés sur des différences de sous ensembles, etc.

5.1 Buts du protocole de changement de clé

Les buts du protocole de changement de clé sont :
- o de synchroniser une GSA,
- o de fournir la protection de la confidentialité, l'authentification (symétrique ou asymétrique), la protection contre la répétition et contre les attaques de déni de service,
- o un changement de clés efficace après des changements de la composition du groupe ou quand les clés (KEK) arrivent à expiration,
- o une livraison fiable des messages de changement de clé,
- o la récupération par un membre d'une GSA désynchronisée,
- o un haut débit et une faible latence,
- o la prise en charge de la diffusion groupée ou de l'envoi individuel multiple sur IP.

On identifie plusieurs problèmes majeurs dans la conception d'un protocole de changement de clé :
1. le format du message de changement de clé,

2. le transport fiable des messages de changement de clé,
3. l' implosion,
4. la récupération d'une GSA désynchronisée,
5. l'incorporation des GKMA dans les messages de changement de clé ,
6. l'interopérabilité des GKMA.

Noter que l'interopération des mises en œuvre de protocole de changement de clé est insuffisante pour qu'un GCKS réussisse à changer les clés d'un groupe. Le GKMA doit aussi interopérer, c'est-à-dire que des versions standard des algorithmes de gestion de clé de groupe comme LKH, OFT, ou Différences de sous ensemble, doivent être utilisés.

Le reste de cette section discute ces sujets en détail.

5.2 Transport et protection du message de changement de clé

Les messages de changement de clé contiennent des SA de changement de clé et/ou de données ainsi que des KEK et des TPK. Ces messages doivent être confidentiels, authentifiés, et protégés contre les attaques en répétition et de déni de service. Ils sont envoyés via diffusion groupée ou envoi individuel multiple du GCKS aux membres.

Les messages de changement de clé sont chiffrés avec la KEK de groupe pour la confidentialité. Quand ils sont utilisés en conjonction avec un GKMA, des portions du message de changement de clé sont d'abord chiffrées avec les KEK appropriées comme spécifié par le GKMA. Le GCKS authentifie les messages de changement de clé en utilisant un MAC, calculé en utilisant la clé d'authentification de groupe, ou une signature numérique. Dans les deux cas, un numéro de séquence est inclus dans le calcul du MAC ou de la signature pour protéger contre les attaques en répétition.

Quand l'authentification du groupe est fournie avec une clé symétrique, les messages de changement de clé sont vulnérables aux attaques par les autres membres du groupe. Les messages de changement de clé sont signés numériquement quand les membres du groupe ne se font pas mutuellement confiance. Quand on utilise une authentification asymétrique, les membres qui reçoivent des messages de changement de clé sont vulnérables aux attaques de déni de service. Un adversaire externe peut envoyer un message de changement de clé bogué, qu'un membre ne pourra pas identifier avant d'avoir effectué une opération coûteuse de vérification de signature numérique. Pour se protéger contre une telle attaque, un MAC peut être envoyé au titre du message de changement de clé. Les membres vérifient la signature seulement si la vérification du MAC a réussi.

Les messages de changement de clé contiennent des mises à jour de clé de groupe qui correspondent à un seul [RFC2627], [OFT] ou à plusieurs changements de membres [SD1], [SD2], [BatchRekey] et peuvent contenir des messages d'initialisation de clés de groupe [OFT].

5.3 Transport fiable des messages de changement de clé

Le GCKS doit s'assurer que tous les membres ont les SA de sécurité des données et de changement de clé actuelles. Autrement, des membres autorisés peuvent être exclus par inadvertance de la réception des communications du groupe. Donc, le GCKS doit utiliser un algorithme de clé qui soit fiable par nature ou employer un mécanisme de transport fiable pour envoyer les messages de changement de clé.

Il y a deux dimensions au problème. Les messages qui mettent à jour les clés de groupe peuvent être perdus dans le transit ou peuvent être manqués par un hôte lorsque il se trouve hors ligne. Les algorithmes LKH et OFT de gestion de clé de groupe s'appuient sur l'historique des mises à jour reçues par l'hôte. Si l'hôte passe hors ligne, il va devoir resynchroniser son état de clé de groupe quand il revient en ligne ; ceci peut exiger un échange en envoi individuel avec le GCKS. L'algorithme "Différence de sous ensemble" porte cependant tout l'état nécessaire dans ses messages de changement de clé et n'a pas besoin que les membres soient toujours en ligne ou gardent l'état. L'algorithme "Différence de sous ensemble" n'exige pas de canal de retour et peut fonctionner sur un réseau de diffusion. Si un message de changement de clé est perdu dans la transmission, l'algorithme "Différence de sous ensemble" ne peut pas déchiffrer les messages chiffrés avec la TPK envoyée via le message de changement de clé perdu. Il y a des GKMA auto réparateurs qui sont proposés dans la littérature qui permettent à un membre de récupérer les messages de changement de clé perdus, pourvu que les messages de changement de clé avant et après le message de changement de clé perdus soient reçus.

Les messages de changement de clé sont normalement courts (pour un seul changement de membre ainsi que pour de petits groupes) qui rendent facile de concevoir un protocole de livraison fiable. D'un autre côté, les exigences de sécurité peuvent ajouter une dimension supplémentaire à traiter. Il y a des cas particuliers dans lesquels des changements des membres sont

traités en bloc, réduisant la fréquence des messages de changement de clé mais augmentant leur taille. De plus, parmi toutes les KEK envoyées dans un message de changement de clé, la moitié des membres ont seulement besoin d'une seule KEK. On peut tirer parti de ces propriétés pour concevoir des messages de changement de clé et un protocole pour leur livraison fiable.

Trois catégories de solutions ont été proposées :
1. Transmettre de façon répétée le message de changement de clé. Dans de nombreux cas, les messages de changement de clé se traduisent en seulement un ou deux paquets IP.
2. Utiliser un protocole/infrastructure existant fiable de diffusion groupée.
3. Utiliser la FEC pour coder les paquets de changement de clé (avec des NACK comme retour) [BatchRekey].

Noter que pour les petits messages, la catégorie 3 est essentiellement la même que la catégorie 1.

Le membre du groupe peut être désynchronisé avec le GCKS si il reçoit un message de changement de clé qui a un numéro de séquence supérieur de un au dernier numéro de séquence traité. C'est un des moyens par lesquels le membre GCKS détecte qu'il a manqué un message de changement de clé. Autrement, l'application de sécurité des données, lorsque elle détecte qu'elle utilise une clé périmée, peut le notifier au module de gestion de clé de groupe. L'action effectuée par le membre GCKS est l'affaire de la politique de groupe. Le membre GCKS devrait enregistrer la condition et peut contacter le GCKS pour qu'il relance le protocole d'enregistrement pour obtenir une clé de groupe fraîche. La politique du groupe doit tenir compte des conditions limites, car des messages de changement de clé réordonnées dans un changement de clés sont si fréquents que deux messages peuvent être réordonnés dans un réseau IP. La politique de clé de groupe doit aussi tenir compte du potentiel d'attaques de déni de service où un attaquant retarde ou supprime un message de changement de clé afin de forcer un sous réseau ou un sous ensemble des membres à contacter simultanément le GCKS.

Si un membre du groupe devient désynchronisé avec la GSA, il devrait alors se réenregistrer auprès du GCKS. Cependant, dans de nombreux cas, il y a d'autres méthodes plus simples pour se resynchroniser avec le groupe :

- Le membre peut ouvrir une simple connexion non protégée (par exemple, TCP) avec le GCKS et obtenir les messages de changement de clé actuels (ou plusieurs messages récents). Noter qu'il n'est pas besoin ici d'authentification ou de chiffrement, car le message de changement de clé est déjà signé et est en clair dans la diffusion groupée. On peut penser que cela ouvre le GCKS à des attaques de DoS par de nombreuses demandes boguées. Cela ne semble cependant pas empirer la situation ; en fait, bombarder le GCKS de demandes de resynchronisation boguées serait plus problématique.

- Le GCKS peut envoyer le messages de changement de clé sur un site public (par exemple, un site de la Toile) et le membre désynchronisé peut obtenir les messages de changement de clé à partir de ce site.

Le GCKS peut toujours fournir les trois façons de se resynchroniser (c'est-à-dire, le réenregistrement, TCP simple, et l'envoi public). De cette façon, le membre peut choisir comment se resynchroniser ; il évite aussi d'ajouter encore un autre champ au jeton de politique [GSPT]. Autrrment, un jeton de politique peut contenir un champ spécifiant une ou plusieurs méthodes prises en charge pour la resynchronisation d'une GSA.

5.4 État de l'art de l'infrastructure fiable de diffusion groupée

Le message de changement de clé peut être envoyé en utilisant une diffusion groupée fiable. Il y a plusieurs types de protocoles de diffusion groupée fiable avec des propriétés différentes. Cependant, il n'y a pas pour l'instant de protocole de diffusion groupée fiable sur la voie de la normalisation publié, bien que le consensus de l'IETF ait été obtenu sur deux protocoles qui sont destinés à aller sur la voie de la normalisation [RFC3450], [RFC3940]. Donc, le présent document ne recommande pas de protocole ou ensemble de protocoles de diffusion groupée fiable particulier pour les besoins du changement de clé de groupe fiable. La convenance des méthodes de diffusion groupée fiable fondée sur le NAK, le ACK, ou autres est déterminée par les besoins de l'application et l'environnement de fonctionnement. À l'avenir, les protocoles de gestion de clé de groupe pourront choisir d'utiliser des approches particulières fondées sur des normes qui satisfont aux besoins des applications particulières. Une facilité d'annonces sécurisées peut être nécessaire pour signaler l'utilisation d'un protocole de diffusion groupée fiable, qui pourrait être spécifié au titre de la politique de groupe. La spécification de politique et d'annonce en diffusion groupé fiable ne peut cependant que suivre l'établissement de normes de diffusion groupée fiable et n'est pas examinée plus avant dans le présent document.

Aujourd'hui, les divers protocoles MSEC de gestion de clé de groupe prennent en charge le séquençage des messages de changement de clé à travers un numéro de séquence, qui est authentifié avec le message de changement de clé. Un envoyeur de messages de changement de clé peut retransmettre de multiples copies du message pourvu qu'ils aient le même numéro de séquence. Donc, envoyer à nouveau le message est un moyen rudimentaire de surmonter la perte sur le chemin

du réseau. Un membre qui reçoit le message de changement de clé va vérifier le numéro de séquence pour détecter les messages de changement de clé dupliqués et manquants. Le membre receveur va éliminer les messages dupliqués qu'il reçoit. Les grands messages de changement de clé, comme ceux qui contiennent des structures d'arborescence de LKH ou OFT, pourront à l'avenir tirer parti de la FEC de couche transport, quand des méthodes normalisées seront disponibles. Il est peu probable que les méthodes de correction d'erreur directe (FEC) bénéficient aux messages de changement de clé courts qui tiennent dans un seul message. Dans ce cas, la FEC dégénère en une simple retransmission du message.

5.5 Implosion

Une implosion peut se produire pour deux raisons. D'abord, on se rappelle qu'un des buts du protocole de changement de clé est de synchroniser une GSA. Quand une SA de changement de clé ou une SA de données arrive à expiration, les membres peuvent contacter le GCKS pour une mise à jour. Si tous les membres, ou même beaucoup d'entre eux, contactent le GCKS à peu près en même temps, le GCKS pourrait n'être pas capable de traiter tous ces messages. On appelle cela une implosion de désynchronisation.
Le second cas est dans la livraison fiable des messages de changement de clé. Les protocoles de diffusion groupée fiable utilisent un retour (NACK ou ACK) pour déterminer quels paquets doivent être retransmis. Des pertes de paquet peuvent résulter en ce que de nombreux membres envoient des NACK au GCKS. On appelle cela une implosion de retours.

Le problème de l'implosion a été étudié extensivement dans le contexte de la diffusion groupée fiable. La suppression proposée du retour et des solutions d'agrégation peuvent aussi être utiles dans le contexte de GKM. Les membres peuvent attendre pendant un délai aléatoire avant d'envoyer un message de retour de désynchronisation. Pendant ce temps, les membres peuvent recevoir les mises à jour de clé nécessaires et donc ne pas envoyer de message de retour. Une solution de remplacement est de faire que les membres contactent un des serveurs d'enregistrement quand ils sont désynchronisés. Cela exige la synchronization des GSA entre les multiples serveurs d'enregistrement.

L'agrégation de retours et la récupération locale employées par certains protocoles de diffusion groupée fiable ne sont pas facilement adaptables au transport des messages de changement de clé. L'agrégation soulève des problèmes d'authentification. La récupération locale est plus complexe parce que les membres ont besoin d'établir des SA avec le serveur local de réparation. Tout membre du groupe ou un GCKS subordonné peut servir de serveur de réparation, qui peut être responsable du renvoi des messages de changement de clé.

Les membres peuvent utiliser la SA de groupe, plus précisément la SA de changement de clés, pour authentifier les demandes envoyées au serveur de réparation. Cependant, la protection contre la répétition exige de conserver l'état chez les membres ainsi que chez les serveurs de réparation. L'authentification des demandes de réparation est destinée à protéger contre les attaques de DoS. Noter aussi qu'un membre désynchronisé peut utiliser une SA de changement de clés expirée pour authentifier des demandes de réparation, ce qui exige que les serveurs de réparation acceptent les messages protégés par les vieilles SA.

Autrement, un mécanisme simple peut être employé pour réaliser efficacement une réparation en local. Chaque membre reçoit un ensemble d'adresses de serveur de réparation local au titre des informations de politique de fonctionnement du groupe. Quand un membre ne reçoit pas de message de changement de clé, il peut envoyer un ou des messages "Retransmettre le ou les messages répétés avec le numéro de séquence n et au -dessus" à un des serveurs de réparation locaux. Le serveur de réparation peut soit ignorer la demande si il est occupé, soit retransmettre les messages de changement de clé demandés comme ils ont été reçus du GCKS. Le serveur de réparation, qui est aussi un autre membre, peut choisir de servir seulement les demandes dans un certain délai (c'est-à-dire, une limite de taux de réponses) ou pour un certain message de changement de clé. La limitation du taux de demandes et de réponses protège les serveurs de réparation ainsi que les autres membres du groupe contre les attaques de DoS.

5.6 Incorporation d'algorithmes de gestion de clé de groupe

Les algorithmes de gestion de clé de groupe (GKMA) rendent le changement de clés adaptable. Les grands groupes qui changent de clé sans employer les GKMA sont d'un coût prohibitif.

Quelques considérations sur le choix d'un GKMA suivent :

o Protection contre la collusion.
Les membres (ou les non membres) ne devraient pas être capables de collaborer pour déduire les clés pour lesquelles ils n'ont pas de privilège (suivant les règles de distribution des clés de GKMA).

o Contrôle d'accès vers l'avant.
Le GKMA devrait s'assurer que les membres qui partent ne peuvent pas obtenir l'accès aux futures données du groupe.

o Contrôle d'accès vers l'arrière.
Le GKMA devrait s'assurer que les membres qui se joignent au groupe ne peuvent pas déchiffrer les données passées.

5.7 Algorithmes de changement de clé sans état, à états pleins, et auto correcteurs

On classe les algorithmes de gestion de clé de groupe en trois catégories : à état pleins, sans état, et auto correcteurs.

Les algorithmes à états pleins [RFC2627], [OFT] utilisent les KEK à partir des instances passées de changement de clés pour chiffrer (protéger) les KEK qui correspondent aux instances courantes et futures de changement de clés. Le principal inconvénient de ces schémas est que si un membre est hors ligne ou échoue autrement à recevoir les KEK d'une instance passée de changement de clés, il ne peut plus être capable de synchroniser sa GSA même si il peut recevoir les KEK de toutes les instances futures de changement de clés. La seule solution est de contacter le GCKS explicitement pour une resynchronisation. Noter que les KEK pour la première instance de changement de clés sont protégées par la SA d'enregistrement. On se rappelle que la communication dans cette phase est de un à un, et donc il est aisé de s'assurer une livraison fiable.

Les algorithmes sans état [SD1], [SD2] chiffrent les messages de changement de clé avec des KEK envoyées durant le protocole d'enregistrement. Comme les messages de changement de clé sont indépendants de tous messages de changement de clé passés (c'est-à-dire, qui ne sont pas protégés par les KEK qui y sont contenues) un membre peut passer hors ligne mais continuer de déchiffrer les futures communications. Cependant, les GKMA sans état n'offrent pas de mécanisme pour récupérer les messages de changement de clé passés. Le changement de clé sans état peut être relativement inefficace, en particulier pour le changement de clé immédiat (pas par lots) dans des groupes très dynamiques.

Dans des schémas auto correcteurs [Self-Healing], un membre peut reconstruire un message de changement de clé perdu pour autant qu'il reçoive quelques messages de changement de clé passés et futurs.

5.8 Interopérabilité d'un GKMA

La plupart des spécifications de GKMA ne spécifient pas de formats de paquet, bien que de nombreux algorithmes de gestion de clé de groupe aient besoin de spécification de format pour l'interopérabilité. Il y a plusieurs façons de gérer les arborescences de clés et de numéroter les nœuds au sein de ces arborescences de clés. Les informations suivantes sont nécessaires durant l'initialisation d'une SA de changement de clés ou sont incluses dans chaque paquet de GKMA :

- o nom du GKMA (par exemple, LKH, OFT, Différence de sous ensemble) ;
- o numéro de version du GKMA (spécifique de la mise en œuvre). La version peut impliquer plusieurs choses comme le degré d'une arborescence de clés, des améliorations brevetées, et qualifier un autre champ comme un identifiant de clé ;
- o nombre de clés ou plus grand identifiant ;
- o données spécifiques de la version ;
- o informations par clé :
  - identifiant de clé,
  - durée de vie de la clé (données de création/expiration),
  - clé chiffrée,
  - identifiant de la clé de chiffrement (facultatif).

Les identifiants de clé peuvent changer dans certaines mises en œuvre et dans ce cas on doit envoyer une liste des paires <vieil identifiant, nouvel identifiant>.

6. Association de sécurité de groupe

L'architecture de GKM définit les interfaces entre les protocoles d'enregistrement, de changement de clé, et de sécurité des données en termes d'associations de sécurité (SA, *Security Association*) de ces protocoles. En isolant ces protocoles derrière une interface uniforme, l'architecture permet aux mises en œuvre d'utiliser le protocole qui convient le mieux à leurs besoins. Par exemple, un protocole de changement de clé pour un petit groupe pourrait utiliser plusieurs transmissions en envoi individuel avec une authentification symétrique, tandis qu'un protocole de changement de clé pour un grand groupe pourrait utiliser la diffusion groupée IP avec la correction d'erreur directe au niveau du paquet et l'authentification de source.

L'architecture de gestion de clé de groupe fournit une interface entre les protocoles de sécurité et la SA de groupe (GSA). La GSA consiste en trois SA : SA d'enregistrement, SA de changement de clés, et SA de données. La SA de changement de clés est facultative. Il y a deux cas de définition des relations entre les trois SA. Dans les deux cas, la SA d'enregistrement protège le protocole d'enregistrement.

Cas 1 : la gestion de clé de groupe est faite SANS utiliser de SA de changement de clés. Le protocole d'enregistrement initialise et met à jour une ou plusieurs SA de données (en ayant des TPK pour protéger les fichiers ou flux). Chaque SA de données correspond à un seul groupe, qui peut avoir plus d'une SA de données.

Cas 2 : la gestion de clé de groupe est faite AVEC une SA de changement de clés pour protéger le protocole de changement de clé. Le protocole d'enregistrement initialise la ou les SA de changement de clé ainsi que zéro, une ou plusieurs SA de données, quand l'achèvement est un succès. Quand une SA de données n'est pas initialisée dans le protocole d'enregistrement, l'initialisation est faite dans le protocole de changement de clé. Le protocole de changement de clé met à jour la ou les SA de changement de clés ET établit la ou les SA de données.

6.1 Politique de groupe

La politique de groupe est décrite en détails dans le document "Jeton de politique de sécurité de groupe" [GSPT]. La politique de groupe peut être distribuée par des annonces de groupe, des protocoles de gestion de clé, et autres moyens hors bande (par exemple, via une page de la Toile). Le protocole de gestion de clé de groupe porte des politiques de chiffrement des SA et des clés qu'il établit, ainsi que des politiques supplémentaires pour le fonctionnement sûr du groupe.

Les politiques de chiffrement acceptables pour le protocole d'enregistrement, qui peuvent fonctionner avec TLS {RFC2246], IPsec, ou IKE, ne sont pas portées dans le protocole de gestion de clé de groupe car elles précèdent tous les échanges de gestion de clé. Donc, un répertoire de politique de sécurité qui a un protocole d'accès peut avoir besoin d'être interrogé avant d'établir la session de gestion de clé, pour déterminer les politiques de chiffrement initiales pour cet établissement. Le présent document suppose l'existence d'un tel répertoire et protocole pour GCKS et les interrogations de politique des membres. Donc la politique de sécurité du groupe va être représentée dans un répertoire de politique et accessible en utilisant un protocole de politique. La distribution de la politique peut être poussée ou tirée.

L'architecture de gestion de clé de groupe suppose que les informations de politique de groupe suivantes peuvent être gérées en externe, par exemple, par le propriétaire du contenu, l'administrateur de conférence ou le propriétaire du groupe :
- o l'identité du propriétaire du groupe, la méthode d'authentification, et la méthode de délégation pour identifier un GCKS pour le groupe ;
- o le GCKS du groupe, la méthode d'authentification, et la méthode de délégation pour tous les GCKS subordonnés pour le groupe ;
- o les règles d'appartenance au groupe ou la liste des membres et la méthode d'authentification.

Il y a deux exigences supplémentaires en relation avec la politique qui sont externes à la gestion de clé de groupe :
- o Il y a une infrastructure d'authentification et d'autorisation comme X.509 [RFC3280], SPKI [RFC2693], ou schéma de clé pré partagée, en accord avec la politiques de groupe pour un groupe particulier.
- o Il y a un mécanisme d'annonces pour les groupes et événements sécurisés, qui opère selon la politique de groupe pour un groupe particulier.

La politique de groupe détermine comment les protocoles d'enregistrement et de changement de clé initialisent ou mettent à jour les SA de changement de clé et de données. Les paragraphes qui suivent décrivent les informations éventuellement envoyées par le GCKS pour les SA de changement de clé et les SA de données. Un membre a besoin des informations spécifiées dans les prochains paragraphes pour établir les SA de changement de clé et les SA de données.

6.2 Contenu de la SA Rekey

La SA de changement de clés protège le protocole de changement de clé. Elle contient la politique de chiffrement, l'identité de groupe, et l'indice de paramètre de sécurité (SPI, *Security Parameter Index*) [RFC2401] pour identifier une SA de façon univoque, les informations de protection contre la répétition, et les clés de protection de clés.

6.2.1 Politique de SA Rekey

- o Algorithme de gestion de clé de groupe

Cela représente l'algorithme de révocation de clé de groupe qui applique le contrôle d'accès vers l'avant et vers l'arrière. Des exemples d'algorithmes de révocation de clés incluent LKH, LKH+, OFT, OFC, et "Différence de sous ensemble" [RFC2627], [OFT], [TAXONOMY], [SD1], [SD2]. Si l'algorithme de révocation de clé est NULL, la SA de changement de clés contient seulement une KEK, qui sert de KEK de groupe. Les messages de changement de clé initialisent ou mettent à jour les SA de données comme d'habitude. Cependant, la SA de changement de clés elle-même peut être mise à jour (la KEK de groupe peut être changée) quand des membres se joignent ou quand la KEK est sur le point d'arriver à expiration. L'abandon du changement de clé est fait en réinitialisant la SA de changement de clés au moyen du protocole de changement de clé.

o Algorithme de chiffrement de KEK
Cela spécifie un algorithme standard de chiffrement comme 3DES ou AES, et aussi la longueur de la clé de KEK.

o Algorithme d'authentification
Cet algorithme utilise des signatures numériques pour l'authentification du GCKS (car tous les secrets partagés sont connus de certains ou de tous les membres du groupe) ou pour certains secrets symétriques dans le calcul des MAC pour l'authentification du groupe. L'authentification symétrique donne une authentification plus faible en ce que tout membre du groupe peut se faire passer pour une source particulière. La longueur de clé d'authentification doit aussi être spécifiée.

o Adresse de groupe de contrôle
Cette adresse est utilisée pour la transmission en diffusion groupée des messages de changement de clé. Ces informations sont envoyées sur le canal de contrôle comme dans un protocole d'annonces ou un message d'établissement d'appel. Le degré de protection de l'adresse de groupe de contrôle relève de la politique du groupe.

o Adresse de serveur de changement de clés
Cette adresse permet au serveur d'enregistrement d'être une entité différente du serveur utilisé pour changer les clés, comme pour de futures invocations des protocoles d'enregistrement et de changement de clé. Si le serveur d'enregistrement et le serveur de changement de clés sont deux entités différentes, le serveur d'enregistrement envoie l'adresse du serveur de changement de clés au titre de la SA de changement de clés.

6.2.2 Identité de groupe

L'identité de groupe accompagne les informations de SA (charge utile) comme un identifiant si le protocole spécifique de gestion de clé de groupe permet que plusieurs groupes soient initialisés dans une seule invocation du protocole d'enregistrement, ou que plusieurs groupes soient mis à jour dans un seul message de changement de clé. Il est souvent plus simple de restreindre chaque invocation d'enregistrement à un seul groupe, maix une telle restriction n'est pas nécessaire. Il est toujours nécessaire d'identifier le groupe lors de l'établissement d'une SA de changement de clés, soit implicitement par un SPI, soit explicitement comme paramètre de SA.

6.2.3 KEK

Correspondant à l'algorithme de gestion de clé, la SA de changement de clés contient une ou plusieurs KEK. Le GCKS détient les clés de chiffrement de clés du groupe, tandis que les membres reçoivent les clés selon la spécification de l'algorithme de gestion de clé. Quand il y a plusieurs KEK pour un groupe (comme dans une arborescence LKH) chaque KEK doit être associée à un identifiant de clé, qui est utilisé pour identifier la clé nécessaire pour la déchiffrer. Chaque KEK a une durée de vie associée, après laquelle la KEK arrive à expiration.

6.2.4 Clés d'authentification

Le GCKS fournit une clé symétrique ou publique pour l'authentification de ses messages de changement de clé. L'authentification par clé symétrique n'est appropriée que quand on peut avoir confiance que tous les membres du groupe ne vont pas se faire passer pour le GCKS. L'architecture n'interdit pas de méthodes pour déduire les clés d'authentification symétriques chez le membre [RFC2409] plutôt que de les pousser à partir du GCKS.

6.2.5 Protection contre la répétition

Les messages de changement de clé doivent être protégés contre les attaques en répétition/réflexion. Les numéros de séquence sont utilisés à cette fin, et la SA de changement de clés (ou le protocole) contient ces informations.

6.2.6 Indice de paramètre de sécurité (SPI)

Le couple <identité de groupe, SPI> identifie de façon univoque une SA de changement de clés. Le SPI change chaque fois que les KEK changent.

6.3 Contenu de la SA Data

Le GCKS spécifie le protocole de sécurité des données utilisé pour la transmission sûre des données de ou des envoyeurs aux membres receveurs. Des exemples de protocoles de sécurité des données incluent IPsec ESP [RFC2401] et SRTP [RFC3711]. Bien que le contenu de chacun de ces protocoles sorte du domaine d'application du présent document, on fait la liste des informations envoyées par le protocole d'enregistrement (ou le protocole de changement de clé) pour initialiser ou mettre à jour la SA de données.

6.3.1 Identité de groupe

L'identité de groupe accompagne les informations de SA quand les SA de données sont initialisées ou que leurs clés sont changées pour plusieurs groupes dans une seule invocation du protocole d'enregistrement ou dans un seul message de changement de clé.

6.3.2 Identité de source

La SA inclut des informations d'identité de source quand le propriétaire du groupe choisit de révéler l'identité de la source aux seuls membres autorisés. Un canal public comme le protocole d'annonces n'est approprié que quand il n'est pas besoin de protéger l'identité de la source ou du groupe.

6.3.3 Clés de protection du trafic

Sans considération du protocole de sécurité des données utilisé, le GCKS fournit les TPK, ou les informations pour déduire les TPK pour la protection du trafic.

6.3.4 Clés d'authentification des données

Selon la méthode d'authentification des données utilisée par le protocole de sécurité des données, la gestion de clé de groupe peut passer une ou plusieurs clés, fonctions (par exemple, TESLA [RFC4082], [TESLA-SPEC]), ou autres paramètres utilisés pour authentifier les flux ou fichiers.

6.3.5 Numéros de séquence

Le GCKS passe les numéros de séquence quand ils sont nécessaires au protocole de sécurité des données, pour la synchronisation des SA et la protection contre la répétition.

6.3.6 Indice de paramètre de sécurité (SPI)

Le GCKS peut fournir un identifiant au titre du contenu de la SA de données pour les protocoles de sécurité des données qui utilisent un SPI ou des mécanismes similaires pour identifier une SA ou des clés au sein d'une SA.

6.3.7. Politique de SA de données

Les paramètres de SA de données sont spécifiques du protocole de sécurité des données mais généralement incluent un algorithme et des paramètres de chiffrement, l'algorithme et les paramètres d'authentification de la source, l'algorithme et les paramètres d'authentification du groupe, et/ou des informations de protection contre la répétition.

7. Considérations d'adaptabilité

Le domaine des communications de groupe est assez divers. Dans la téléconférence, une unité de contrôle multipoint

(MCU, *multipoint control unit*) peut être utilisée pour agréger un certain nombre de membres de la téléconférence dans une seule session ; les MCU peuvent aussi être organisées hiérarchiquement. Une session de téléconférence à couplage lâche [RFC3550] n'a pas de contrôleur central mais est entièrement répartie et de bout en bout. Les sessions de téléconférence tendent à avoir au plus une douzaine de participants. Cependant, la diffusion vidéo qui utilise des communications en diffusion groupée et des supports à la demande qui utilisent l'envoi individuel sont des groupes à grande échelle qui comptent des centaines ou même des millions de participants.

Comme décrit dans la Section 2 "Exigences", l'architecture de gestion de clé de groupe prend en charge les applications de diffusion groupée avec un seul envoyeur. L'architecture décrite dans le présent document prend en charge un fonctionnement à grande échelle avec les caractéristiques suivantes :

1. Il n'est pas nécessaire qu'un échange en envoi individuel fournisse les clés de données à un protocole de sécurité pour les membres préalablement enregistrés dans un certain groupe ; les clés de données peuvent être poussées dans le protocole de changement de clé.
2. Les protocoles d'enregistrement et de changement de clé sont séparables pour donner de la souplesse à la façon dont les membres reçoivent les secrets du groupe. Un groupe peut utiliser un système fondé sur une carte à mémoire à la place du protocole d'enregistrement, par exemple, pour permettre au protocole de changement de clé d'être utilisé sans canal de retour pour les applications de diffusion comme les systèmes de télévision à accès conditionnel.
3. Les protocoles d'enregistrement et de changement de clé prennent en charge de nouvelles clés, algorithmes, mécanismes d'authentification et infrastructures d'autorisation dans l'architecture. Quand l'infrastructure d'autorisation accepte la délégation, comme dans X.509 et SPKI, la fonction de GCKS peut être répartie comme montré à la Figure 3.

La première caractéristique de la liste permet un changement de clés rapide des protocoles de sécurité des données quand le membre appartient déjà au groupe. Alors que ceci est réaliste pour des groupes d'abonnés et consommateurs de fournisseurs de service qui offrent des événements de contenu, cela peut être trop restrictif pour les applications qui permettent l'adhésion du membre au moment de l'événement. L'architecture MSEC de gestion de clé de groupe suggère une distribution de clés organisée hiérarchiquement pour traiter un enregistrement, potentiellement de masse, simultané de demandes. La configuration de la Figure 3 peut être nécessaire quand les solutions conventionnelles de grappe et d'équilibrage de charge d'un site central de GCKS ne peuvent pas satisfaire les exigences des utilisateurs. À la différence des réseaux conventionnels de mise en antémémoire et de distribution de contenu, la configuration de la Figure 3 a des ramifications de sécurité supplémentaires pour la sécurité physique d'un GCKS.

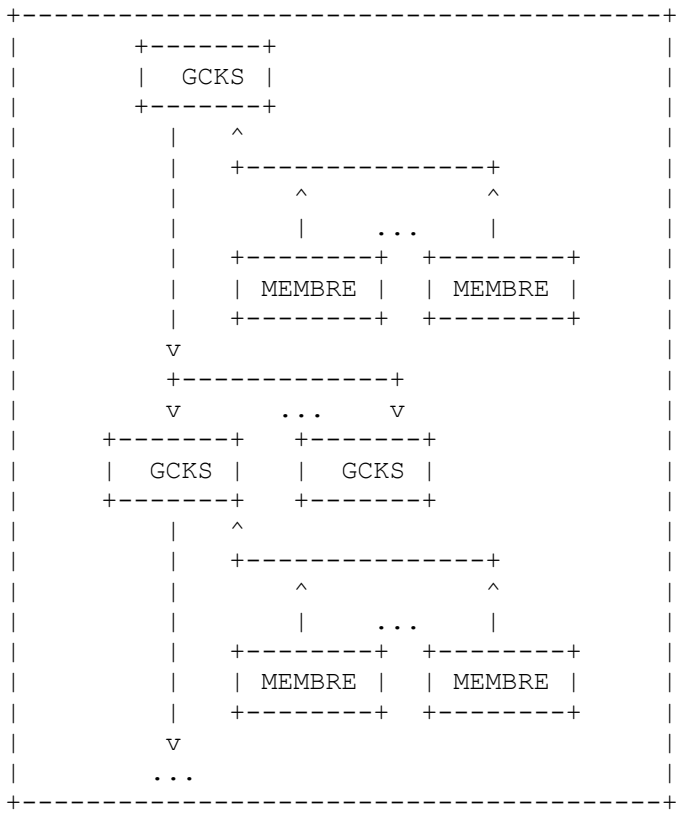


Figure 3 : Distribution hiérarchique de clés

Des analyses et des travaux supplémentaires sont nécessaires sur les instanciations de protocole de l'architecture de gestion de clé de groupe pour déterminer comment l'architecture peut effectivement prendre en charge en toute sécurité les applications de diffusion groupée à grande échelle. En plus d'être aussi sûre que la gestion de clé pair à pair contre les attaques par interposition, en répétition et en réflexion, les protocoles de gestion de clé de groupe ont des besoins de sécurité supplémentaires. À la différence de la gestion de clé pair à pair, la gestion de clé de groupe a besoin d'être sûre contre les attaques par les membres du groupe qui tentent de se faire paser pour un GCKS ou perturber le fonctionnement d'un GCKS, ainsi que par des non membres.

Donc, les groupes sécurisés doivent converger vers une clé de groupe commune quand des membres attaquent le groupe, en se joignant et en quittant le groupe, ou en étant évincés du groupe. Les protocoles de gestion de clé de groupe ont aussi besoin d'être robustes quand des attaques de DoS ou une partition de réseau conduit à de grands nombres de demandes synchronisées. Une instanciation de gestion de clé de groupe, a donc besoin de considérer comment le fonctionnement du GCKS pourrait être réparti entre de multiples GCKS désignés par le propriétaire du groupe pour servir les clés au nom d'un GCKS désigné. Le protocole GSAKMP [RFC4535] utilise le jeton de politique et permet de désigner certains des membres comme GCKS subordonnés pour traiter ce problème d'adaptabilité.

8. Considérations sur la sécurité

Le présent mémoire décrit l'architecture MSEC de gestion de clé. Cette architecture va être instanciée dans un ou plusieurs protocoles de gestion de clé de groupe, qui doivent être protégés contre les attaques par interposition, de capture de connexion, de répétition, ou de réflexion de messages passés, et de déni de service.

Les techniques d'échange de clé authentifiés [STS], [SKEME], [RFC2408], [RFC2412], [RFC2409] limitent les effets des attaques par interposition et de capture de connexion. Les techniques d'authentification de message pas numéros de séquence et faible calcul peuvent être efficaces contre les attaques en répétition et réflexion. Des mouchards [RFC2522], quand ils sont mis en œuvre de façon appropriée, fournissent un moyen efficace pour réduire les effets des attaques de déni de service.

Le présent mémoire ne traite pas des attaques contre les mises en œuvre de protocole de gestion de clé ou de sécurité comme les attaques dites de type qui visent à perturber une mise en œuvre par des moyens comme le débordement de mémoire tampon. Le présent mémoire se concentre sur la sécurisation du protocole, non sur la mise en œuvre du protocole.

Alors que les techniques classiques d'échange de clé authentifié peuvent être appliquées à la gestion de clé de groupe, de nouveaux problèmes surviennent avec le partage de secrets parmi un groupe de membres : les secrets du groupe peuvent être divulgués par un membre du groupe, et d'autres membres du groupe peuvent se faire passer pour les envoyeurs du groupe. Les messages de gestion de clés provenant du GCKS ne devraient pas être authentifiés en utilisant des secrets symétriques partagés sauf si on peut faire confiance à tous les membres du groupe pour ne pas se faire passer pour le GCKS ou pour un autre membre. De même, les membres qui divulguent les secrets du groupe sapent la sécurité du groupe entier. Les propriétaires de groupe et les administrateurs de GCKS doivent être conscients de ces limitations inhérentes à la gestion de clé de groupe.

Une autre limitation de la gestion de clé de groupe est la complexité de la politique. Alors que la politique de sécurité d'homologue à homologue est l'intersection de la politique des homologues individuels, un propriétaire du groupe établit en externe la sécurité du groupe dans les groupes sécurisés. Le présent document suppose qu'il n'y a pas de négociation des paramètres de chiffrement ou autres paramètres de sécurité dans la gestion de clé de groupe. La politique de sécurité du groupe présente donc de nouveaux risques pour les membres qui envoient et reçoivent des données dans des groupes sécurisés. Les administrateurs de la sécurité, les opérateurs de GCKS, et les utilisateurs doivent déterminer les niveaux minimaux acceptables de sécurité (par exemple, la politique d'authentification et d'admission du groupe, les longueurs de clés, les algorithmes et protocoles de chiffrement utilisés) quand ils se joignent à des groupes sécurisés.

Étant donnés les limitations et risques de sécurité du groupe, la sécurité du protocole d'enregistrement de gestion de clé de groupe devrait être aussi bonne que les protocoles de base sur lesquels il est développé, comme IKE, IPsec, TLS, ou SSL. Les instanciations particulières de cette architecture de gestion de clé de groupe doivent s'assurer que les exigences pour l'échange de clé authentifié sont préservées dans leurs spécifications de protocoles, qui devront être des documents sur la voie de la normalisation de l'Internet, soumis à relecture, analyse, et essais.

Le second protocole, le protocole de changement de clé de gestion de clé de groupe, est nouveau et les risques sont inconnus. Les risques de l'authentification de source décrits ci-dessus sont atténués par l'utilisation du chiffrement à clé publique. L'utilisation de la livraison en diffusion groupée peut soulever des problèmes de sécurité supplémentaires tels que

de fiabilité, d'implosion, et d'attaque de déni de service fondée sur l'utilisation de la diffusion groupée. La spécification du protocole de changement de clé doit offrir des solutions sûres à ces problèmes. Chaque instanciation de protocole de changement de clé, comme les opérations Rekey de GSAKMP ou Groupkey-push de GDOI, a besoin de valider la sécurité de ses spécifications de changement de clés.

La nouveauté et la complexité sont les plus gros risques des protocoles de gestion de clé de groupe. Plus d'analyses et d'expérience sont nécessaires pour s'assurer que l'architecture décrite dans ce document peut fournir une norme bien articulée pour la sécurité et les risques de la gestion de clé de groupe.

9. Remerciements

Le projet Internet "GKM Building Block" [GKMBB] du SMuG était un précurseur du présent document ; merci à Thomas Hardjono et Hugh Harney de leurs efforts. Durant le cours de la préparation de ce document, Andrea Colegrove, Brian Weis, George Gross, et plusieurs autres du groupe de travail MSEC et des groupes de recherche GSEC et SMuG ont fourni de précieux commentaires qui ont aidé à améliorer ce document. Les auteurs reconnaissent le prix de leurs contributions à ce document.

10 Références pour information

[BatchRekey] Yang, Y. R., and al., "Reliable Group Rekeying: Design and Performance Analysis", Proc. ACM SIGCOMM, San Diego, CA, août 2001.

[CLIQUES] Steiner, M., Tsudik, G., and M. Waidner, "CLIQUES: A New Approach to Group Key Agreement", IEEE ICDCS 97, mai 1997

[FN93] Fiat, A. and M. Naor, "Broadcast Encryption, Advances in Cryptology", CRYPTO 93 Proceedings, Lecture Notes in Computer Science, Vol. 773, pp. 480-491, 1994.

[GKMBB] Harney, H., M. Baugher, and T. Hardjono, "GKM Building Block: Group Security Association (GSA) Definition," Travail en cours, septembre 2000

[GSPT] Hardjono, T., Harney, H., McDaniel, P., Colegrove, A., and P. Dinsmore, "The MSEC Group Security Policy Token", Travail en cours, août 2003.

[H.235] Recommandation UIT-T H.235, "Sécurité et chiffrement pour terminaux multimédia de la série H (H.323 et autres fondés sur H.245) version 3", Union Internationale des Télécommunications, 2001.

[JKKV94] Just, M., Kranakis, E., Krizanc, D., and P. vanOorschot, "On Key Distribution via True Broadcasting", Proc. 2nd ACM Conference on Computer and Communications Security, pp. 81-88, novembre 1994.

[MARKS] Briscoe, B., "MARKS: Zero Side Effect Multicast Key Management Using Arbitrarily Revealed Key Sequences", Proc. First International Workshop on Networked Group Communication (NGC), Pisa, Italy, novembre 1999.

[MVV] Menzes, A.J., van Oorschot, P.C., and S.A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[OFT] Balenson, D., McGrew, P.C., and A. Sherman, "Key Management for Large Dynamic Groups: One-Way Function Trees and Amortized Initialization", IRTF. Travail en cours, août 2000.

[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.)*

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999. *(P.S. ; MàJ par* RFC7919)

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

[RFC2327] M. Handley et V. Jacobson, "SDP : Protocole de description de session", avril 1998. *(Obsolète; voir* RFC8866)

[RFC2367] D. McDonald, C. Metz, B. Phan, "API de gestion de clé PF_KEY, version 2", juillet 1998. *(Information)*

[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, "Protocole Internet d'association de sécurité et gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

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

[RFC2412] H. Orman, "Protocole OAKLEY de détermination de clés", novembre 1998. *(Information)*

[RFC2522] P. Karn, W. Simpson, "Photuris : Protocole de gestion de clé de session", mars 1999. *(Expérimentale)*

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

[RFC2693] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen, "Théorie des certificats SPKI", septembre 1999. *(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)

[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)

[RFC3450] M. Luby et autres, "Instance de protocole de codage en couches asynchrone (ALC)", décembre 2002. *(Expérimentale, remplacée par* RFC5775)

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

[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)

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

[RFC3740] T. Hardjono et B. Weis, "Architecture de sécurité de groupe de diffusion groupée", mars 2004. *(Information)*

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

[RFC3940] B. Adamson et autres, "Protocole de diffusion groupée fiable (NORM) orientée accusé de réception négatif (NACK)", novembre 2004. *(Expérimentale ; Remplacée par* RFC5740)

[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. *(Information)*

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

[SD1] Naor, D., Naor, M., and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receiver", Advances in Cryptology - CRYPTO, Santa Barbara, CA: Springer-Verlag Inc., LNCS 2139, août 2001.

[SD2] Naor, M. and B. Pinkas, "Efficient Trace and Revoke Schemes", Proceedings of Financial Cryptography 2000, Anguilla, British West Indies, février 2000.

[Self-Healing] Staddon, J., and al., "Self-healing Key Distribution with Revocation", Proc. 2002 IEEE Symposium on Security and Privacy, Oakland, CA, mai 2002.

[SKEME] H. Krawczyk, "SKEME: A Versatile Secure Key Exchange Mechanism for Internet", ISOC Secure Networks and Distributed Systems Symposium, San Diego, 1996.

[STS] Diffie, P., van Oorschot, M., and J. Wiener, "Authentication and Authenticated Key Exchanges", Designs, Codes and Cryptography, 2, 107-125 (1992), Kluwer Academic Publishers.

[TAXONOMY] Canetti, R., and al., "Multicast Security: A Taxonomy and some Efficient Constructions", IEEE INFOCOM, 1999.

[TESLA-SPEC] Perrig, A., R. Canetti, and Whillock, "TESLA: Multicast Source Authentication Transform Specification", Travail en cours, avril 2002.

[tGSAKMP] Harney, H., and al., "Tunneled Group Secure Association protocole de gestion de clé", Travail en cours, mai 2003.

[TPM] Marks, D. and B. Turnbull, "Technical protection measures: The Intersection of Technology, Law, and Commercial Licenses", Workshop on Implementation Issues of the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), World Intellectual Property Organization, Geneva, 6 et 7 décembre 1999.

[Wool] Wool, A., "Key Management for Encrypted broadcast", 5th ACM Conference on Computer and Communications Security, San Francisco, CA, novembre 1998.

Adresse des auteurs

Mark Baugher
Cisco Systems
5510 SW Orchid St.
Portland, OR 97219, USA
tél. : +1 408-853-4418
mél : mbaugher@cisco.com

Ran Canetti
IBM Research
30 Saw Mill River Road
Hawthorne, NY 10532, USA
tél. :+1 914-784-7076
canetti@watson.ibm.com

Lakshminath R. Dondeti
Qualcomm
5775 Morehouse Drive
San Diego, CA 92121
tél. : +1 858 845 1267
ldondeti@qualcomm.com

Fredrik Lindholm
Ericsson Research
SE-16480 Stockholm,
Sweden
tél. : +46 8 58531705
redrik.lindholm@ericsson.com

Déclaration complète de droits de reproduction

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 répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

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

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.