Groupe de travail Réseau
Request for Comments : 2627
Catégorie : Information
Traduction Claude Brière de L'Isle

D. Wallner, E. Harder, R. Agee
National Security Agency
juin 1999

Gestion de clé pour la diffusion groupée : Problèmes et architectures

Statut du présent mémoire

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

Résumé

Le présent rapport contient un exposé du difficile problème de la gestion de clés pour les sessions de communication en diffusion groupée. Il se concentre sur deux principaux domaines de préoccupations par rapport à la gestion de clé qui sont l'initialisation du groupe de diffusion groupée avec une clé réseau commune et le changement de clés du groupe de diffusion groupée. Un changement de clé peut être nécessaire en cas de compromission d'un usager ou pour d'autres raisons (par exemple, un changement périodique). En particulier, le présent rapport identifie une technique qui permet une récupération sûre sur compromission, tout en étant aussi robuste contre la collusion des utilisateurs exclus. C'est une caractéristique importante de la gestion de clés de diffusion groupée qui n'a pas été traitée en détail par la plupart des autres propositions de gestion de clé de diffusion groupée [1], [2], [4]. Les avantages techniques de cette proposition sont qu'elle minimise le nombre de transmissions exigé pour changer les clés du groupe de diffusion groupée et qu'elle impose des exigences minimales de mémorisation au groupe de diffusion groupée.

Table des matières

1. Motifs

Il est reconnu que les futurs réseaux auront des exigences qui vont peser sur les capacités des architectures actuelles de gestion de clé. Une de ces exigences sera celle d'une diffusion groupée sûre. Le besoin d'une forte bande passante, de communications de diffusion groupée sûres très dynamiques est de plus en plus évident dans une grande diversité de communautés commerciales, gouvernementales, et dans celle de l'Internet. Précisément, l'exigence d'une diffusion groupée sûre est la nécessité pour de nombreux utilisateurs qui partagent les mêmes attributs de sécurité et des exigences de communication pour communiquer en toute sécurité avec tous les autres membres du groupe de diffusion groupée en utilisant une clé réseau commune de groupe de diffusion groupée. Le plus grand avantage de la communication en diffusion groupée étant que des receveurs multiples obtiennent simultanément la même transmission. Donc, le problème est de permettre à chaque utilisateur de déterminer/obtenir la même clé réseau sans permettre à des parties non autorisées de faire la même chose (d'initialiser le groupe de diffusion groupée) et de changer en toute sécurité les clés des utilisateurs du groupe de diffusion groupée lorsque nécessaire. À première vue, cela ne semble pas différent des scénarios actuels de

gestion de clé. Cet article va cependant montrer que de futurs scénarios de diffusion groupée auront des exigences très divergentes de changement dynamique qui sont un véritable défi du point de vue de la gestion de clé.

2. Introduction

Les réseaux du futur seront capables de prendre en charge des bandes passantes de l'ordre du gigabit pour les utilisateurs individuels, à de grands groupes d'utilisateurs. Ces usagers auront à leur disposition diverses options de qualité de service et des applications multimédia qui incluent la vidéo, la voix, et les données, toutes sur le même réseau support. Le désir de créer de petits groupes d'utilisateurs tous interconnectés et capables de communiquer les uns avec les autres, mais qui soient isolés en toute sécurité de tous les autres usagers sur le réseau est exprimé fortement par les usagers de diverses communautés.

L'infrastructure de gestion des clés doit prendre en charge des bandes passantes qui vont du kilobit/s au gigabit/s, traiter une gamme de tailles de groupe de diffusion groupée, et être assez souple pour traiter, par exemple, des environnements de communications de technologies sans fil et mobile. En plus de ces exigences de performances et de communications, les exigences de sécurité des différents scénarios couvrent aussi une large gamme. Il est exigé que les usagers puissent être ajoutés et retirés efficacement et en toute sécurité, aussi bien individuellement qu'en bloc. Le système doit être résistant à la compromission, dans la mesure où les usagers qui ont été éliminés ne devraient pas être capables de lire le trafic postérieur à leur éviction, même si ils partagent leurs informations secrètes. Les coûts qu'on cherche à minimiser sont le temps nécessaire à l'établissement, l'espace mémoire pour chaque utilisateur final, et le nombre total de transmissions nécessaire à l'établissement, au changement de clés et la maintenance. Il est aussi envisagé que tout mécanisme de sécurité proposé pour la diffusion groupée ne soit pas mis en œuvre à une couche inférieure avec les caractéristiques de la couche réseau de la pile de protocoles. L'efficacité de la bande passante pour tout système de gestion de clés doit aussi être prise en considération. Le compromis entre sécurité et performances de l'ensemble de l'établissement de la session de diffusion groupée sera discuté plus en détail plus loin.

La section suivante explique plusieurs scénarios potentiels où les capacités de diffusion groupée peuvent être nécessaires, et elle quantifie leurs exigences à la fois du point de vue des performances et de la sécurité. Elle sera suivie à la Section 4 par une liste des facteurs qu'on doit considérer lors de la conception d'une solution potentielle. Bien que plusieurs services de sécurité soit examinés ici où là dans le présent document, celui-ci s'est surtout concentré sur la génération et la distribution des clés réseau de groupe de diffusion groupée. On suppose que tous les participants potentiels de la diffusion groupée ont reçu le matériel de clé d'initialisation (par exemple, des certificats) par un mécanisme manuel ou automatisé, centralisé ou décentralisé. Le présent document ne traite pas des questions de distribution des clés d'initialisation. La Section 5 détaille ensuite plusieurs architectures potentielles de gestion de clé de diffusion groupée, de clés manuelles (symétrique) et publiques (asymétrique) et met en lumière leurs avantages et inconvénients relatifs. (Noter que la liste des avantages et inconvénients n'est en aucune façon exhaustive.). En particulier, cette section insiste sur une technique qui permet une récupération sûre d'une situation de compromission.

3. Scénarios de diffusion groupée

Divers scénarios potentiels sous-tendent l'infrastructure de gestion de clé. Ces scénarios incluent, mais ne s'y limitent pas, les jeux de guerre, l'application de la loi, la téléconférence, la commande et le contrôle de conférence, le soulagement des désastres, et l'informatique répartie. Les exigences potentielles de performances et de sécurité, en particulier en termes de groupes de diffusion groupée qui peuvent être formés par ces utilisateurs pour chaque scénario, consistent en la taille potentielle du groupe de diffusion groupée, en exigences d'initialisation (à quelle vitesse les utilisateurs ont besoin d'être mis en ligne) en exigences d'ajout et de suppression (à quelle vitesse un usager doit-il être ajouté ou supprimé du groupe de diffusion groupée à la suite de l'initialisation) en la dynamique de taille (le nombre relatif de gens qui se joignent/quittent ces groupes par unité de temps) en exigences de sécurité de haut niveau, et en questions particulières diverses pour chaque scénario. Alors que certains scénarios décrivent des exigences futures de diffusion groupée sûre, d'autres ont des besoins de sécurité immédiats.

Par exemple, considérons deux scénarios, les jeux répartis et la téléconférence.
Les jeux répartis ont à voir avec le besoin des gouvernements de simuler un scénario de conflit pour des besoins d'entraînement et d'évaluation. En plus des équipements de communications réels utilisés, ce concept inclurait une interconnexion massive de simulations informatiques contenant, par exemple, des visioconférences et du traitement d'image. Le jeu réparti peut être plus exigeant du point de vue de la gestion de clés qu'un scénario réel, pour plusieurs raisons. D'abord, les nœuds du réseau de simulation peuvent être dispersés à travers tout le pays. Ensuite des communications à très grosse bande passante, qui donnent la possibilité de capacités de simulation en temps réel, vont conduire au besoin d'éliminer rapidement des usagers hors de la simulation. C'est potentiellement le scénario le plus exigeant de tous ceux considérés.

Ce scénario peut impliquer des tailles de groupe d'éventuellement 1000 participants ou plus, dont certains peuvent être collectés dans de plus petits sous-groupes. Ces groupes doivent être constitués très rapidement, par exemple, dans un temps total d'initialisation d'un dizième de seconde. Ce scénario est aussi très exigeant en ce que les usagers doivent être ajoutés ou supprimés du groupe en l'espace d'une seconde. Du point de vue de la dynamique des tailles, on estime qu'approximativement dix pour cent des membres du groupe peuvent changer en l'espace d'une minute. Les exigences de taux des données sont larges, allant de quelques kilobits par seconde (pour la simulation d'utilisateurs tactiques) au gigabit par seconde (vidéo en diffusion groupée). Le scénario de jeu réparti a un ensemble d'exigences de sécurité extrêmement serré qui couvre le contrôle d'accès, l'authentification d'usager à usager, la confidentialité des données, et l'intégrité des données. Il doit aussi être "robuste" ce qui implique de traiter des environnements bruyants qui sont typiques de certains appareils tactiques. Finalement, la notion de disponibilité est appliquée à ce scénario, et elle implique que le réseau de communications qui fournit la capacité de diffusion groupée doit être apte à fonctionner un pourcentage spécifié du temps.

Le scénario de la téléconférence peut impliquer des tailles de groupe d'éventuellement 1000 participants ou plus. Ces groupes peuvent prendre jusqu'à plusieurs minutes à initialiser. Ce scénario est moins exigeant en ce que les usagers doivent pouvoir être ajoutés au groupe ou supprimés en quelques secondes. Du point de vue de la dynamique des tailles, on estime qu'approximativement dix pour cent des membres du groupe peuvent changer en quelques minutes. Les exigence de taux des données sont larges, allant de quelques kilobits par seconde à des centaines de Mbit par seconde. Le scénario de la téléconférence a aussi un ensemble d'exigences de sécurité très serré qui couvre le contrôle d'accès, l'authentification d'usager à usager, la confidentialité des données, l'intégrité des données et la non répudiation. La notion de disponibilité est aussi applicable à ce scénario. L'échéance à laquelle ce scénario doit être fourni est 'maintenant'.

4. Questions architecturales

Il y a de nombreux facteurs qui doivent être pris en compte quand on développe l'architecture de gestion de clés désirée. Les questions importantes pour les architectures de gestion de clé incluent le niveau de sécurité (la force) le coût, l'initialisation du système, les questions de politique, les procédures de contrôle d'accès, les exigences de performance et les mécanismes de prise en charge. De plus, les questions particulières aux groupes de diffusion groupée incluent :

1. Que sont les exigences de sécurité des membres du groupe ? Très vraisemblablement il y aura un ou des contrôleurs de groupe. Les autres membres possèdent-ils les mêmes exigences de sécurité que le ou les contrôleurs ?
2. Questions d'interdomaine – Quand on passe d'un "domaine de groupe" à un autre domaine qui a éventuellement une politique de sécurité différente, quelle politique s'applique ? Un exemple serait celui de deux usagers qui souhaitent communiquer, mais qui ont des politiques de périodes de chiffrement et/ou de longueur de clé différentes.
3. Comment se fait la formation du groupe de diffusion groupée ? Est-ce le contrôleur de groupe qui initie le processus d'adjonction des usagers, où bien les usagers qui ont l'initiative du moment où ils se joignent à la formation du groupe de diffusion groupée ?
4. Comment traite t-on le cas où certains membres du groupe ont des capacités de traitement inférieures qui pourraient retarder la formation de la clé réseau ? Ces usagers retardent-ils la formation de l'ensemble du groupe de diffusion groupée, ou viennent-ils en ligne plus tard, permettant aux participants restants d'être constitués en groupe plus rapidement ?
5. On doit minimiser le nombre de bits requis pour la distribution de clé réseau de groupe de diffusion groupée. Cela a un gros impact sur les équipements à bande passante limitée.

Tout cela, et d'autres questions, doit être pris en compte, ainsi que les protocoles de communication qui seront utilisés pour prendre en charge la capacité de diffusion groupée désirée. La section suivante traite certaines de ces questions et présente des architectures candidates qui pourraient être utilisées pour s'attaquer au problème de la gestion de clés pour la diffusion groupée.

5. Architectures candidates

Plusieurs fonctions de base doivent être assurées pour que se réalise une session de diffusion groupée sûre. L'ordre dans lequel ces fonctions seront assurées, et l'efficacité de la solution globale résulte des transactions entre les divers facteurs énumérés ci-dessus. Avant d'examiner les spécificités de chaque architecture, on va préciser ces fonctions de base, ainsi que quelques définition de termes qui seront utilisés dans les architectures représentatives. Ces définitions et fonctions sont les suivantes :

1. Quelqu'un détermine le besoin d'une session de diffusion groupée, règle les attributs de sécurité pour cette session (par exemple, les niveaux de classement du trafic, les algorithmes à utiliser, les longueurs des clés binaires variables, etc.) et crée la liste de contrôle d'accès au groupe qu'on appellera la liste initiale des participants au groupe de diffusion

groupée. L'entité qui effectue ces fonctions sera appelée l'initiateur. À ce moment, la liste des participants au groupe de diffusion groupée est strictement une liste d'usagers que l'initiateur veut introduire dans le groupe de diffusion groupée.

2. L'initiateur détermine qui va contrôler le groupe de diffusion groupée. Ce contrôleur sera appelé la racine (ou de façon équivalente, le serveur). Souvent, l'initiateur va devenir la racine, mais il existe une possibilité que ce contrôle soit passé à quelqu'un d'autre que l'initiateur. (Certaines architectures de gestion de clés emploient plusieurs racines, voir [4]). Le travail de la racine est d'effectuer les ajouts et suppressions de participants au groupe, d'effectuer le contrôle d'accès des utilisateurs par rapport aux attributs de sécurité de cette session, et de distribuer la clé de chiffrement de trafic pour la session et que nous appellerons la clé réseau du groupe de diffusion groupée. Après l'initialisation, l'entité qui a l'autorité pour accepter ou rejeter l'ajout des futurs participants au groupe, ou de supprimer les participants actuels au groupe est appelée le contrôleur de liste.

   Cela peut être ou non l'initiateur. Le contrôleur de liste a été distingué de la racine pour des raisons qui seront précisées plus loin. En bref, il peut être souhaitable que quelqu'un ait l'autorité pour accepter ou rejeter les nouveaux membres, tandis qu'une autre partie (la racine) va effectuer réellement la fonction.
3. Tout participant à la session de diffusion groupée sera appelé un participant au groupe. Des participants au groupe spécifiques autres que la racine ou le contrôleur de liste seront appelés les feuilles.
4. Après que la racine a vérifié les attributs de sécurité des participants énumérés sur la liste des participants au groupe de diffusion groupée pour s'assurer qu'ils prennent tous en charge les attributs de sécurité requis, la racine va alors passer la liste du groupe de diffusion groupée à tous les autres participants et créer et distribuer la clé réseau. Si un participant figurant sur la liste du groupe de diffusion groupée ne satisfait pas aux attributs de sécurité requis, la feuille doit être supprimée de la liste.

Plusieurs problèmes peuvent être soulevés à propos de la distribution de la liste et de la clé réseau du groupe de diffusion groupée.

a. Il se pose une question sur l'ordonnancement de ces fonctions. La liste du groupe de diffusion groupée pourrait être distribuée avant ou après que la liaison est sécurisée (c'est-à-dire, que la clé réseau est distribuée).

b. Un problème se pose lorsque une feuille refuse de se joindre à la session. Si cela se produit, on peut envoyer une liste modifiée avant d'envoyer la clé réseau, cependant, l'envoi de listes modifiées, éventuellement plusieurs fois, serait inefficace. À la place, la racine pourrait continuer et ne pas envoyer la clé réseau aux participants inscrits sur la liste qui ont rejeté la session.

Pour les scénarios d'architectures qui suivent, on suppose que la liste du groupe de diffusion groupée sera distribuée aux participants au groupe une seule fois avant la distribution de la clé réseau. À la différence du schéma décrit dans [4], on recommande que la liste des participants au groupe de diffusion groupée soit fournie à toutes les feuilles. En distribuant cette liste à toutes les feuilles, il leur permet alors de déterminer à l'avance si elles désirent participer ou non au groupe de diffusion groupée, faisant l'économie d'échanges de clé potentiellement inutiles.

On présente quatre architectures potentielles de gestion de clés pour distribuer le matériel de clés pour session de diffusion groupées. On rappelle que les caractéristiques qu'il est très souhaitable que possède l'architecture incluent le temps requis pour l'établissement du groupe de diffusion groupée qui devrait être minimisé, le nombre de transmissions qui devrait être minimisé, et des exigences de mémoire/stockage qui devraient être minimisées. Comme on le verra, les trois premières propositions ne satisfont pas un des différents aspects des trois qualités désirées, tandis que la quatrième proposition paraît tenir l'équilibre entre les caractéristiques désirées. Donc, la quatrième proposition est recommandée pour une mise en œuvre et utilisation générale.

Prière de noter que ces approches visent aussi l'élimination sûre d'utilisateurs du groupe de diffusion groupée, mais ne visent pas spécifiquement l'ajout de nouveaux utilisateurs au groupe de diffusion groupée après l'établissement initial parce que la façon de le faire paraît évidente.

5.1 Distribution manuelle de clés

Par une distribution de clés manuelle, une clé symétrique est délivrée sans utilisation d'échange de clé publique. L'établissement de la clé réseau d'un groupe de diffusion groupée en utilisant une distribution de clé manuelle exigerait une séquence d'événements où la clé réseau et des clés réseau de rechange seraient ordonnées par la racine du groupe de session de diffusion groupée. Les clés réseau de remplacement (supersession) sont ordonnées par la racine pour être utilisées en cas de compromission d'un ou de participants au groupe. Les clés réseau seraient distribuées à chaque participant individuel au groupe, souvent par une localisation physique intermédiaire centralisée. À un moment prédéterminé, tous les participants au groupe vont passer à la nouvelle clé réseau. Les participants au groupe utilisent cette clé réseau jusqu'à un instant prédéterminé auquel ils ont besoin d'une autre nouvelle clé réseau. Si la clé réseau est

compromise pendant ce temps, la clé réseau de remplacement est utilisée. Les participants au groupe passent à la clé réseau de remplacement aussitôt qu'ils la reçoivent, ou sur notification de la racine que tout le monde a la nouvelle clé réseau et que donc la commutation devrait avoir lieu. Cette procédure est répétée pour chaque période de chiffrement.

Un tel schéma peut plaire parce que la méthode existe aujourd'hui et qu'elle est comprise pas les usagers. Malheureusement, ce type de schéma peut être gros consommateur de temps pour établir le groupe de diffusion groupée sur la base du temps nécessaire pour ranger le matériel de clé et le faire livrer. Pour la plupart des scénarios de temps réel, cette méthode est beaucoup trop lente.

5.2 Approche avec N clés par paire racine/feuille

Cette approche est une méthode brutale pour fournir une clé réseau commune de groupe de diffusion groupée aux participants au groupe. Dans ce schéma, l'initiateur établit les attributs de sécurité pour une certaine session, il génère une liste des participants désirés pour le groupe et transmet la liste à tous les participants au groupe. Les feuilles répondent alors par une acceptation initiale ou un rejet de participation. Par l'envoi de la liste à l'avance, on peut gagner du temps à ne pas effectuer d'échange de clés avec les gens qui ont décliné l'offre de participation à la session. La racine (qui pour cet exemple et les suivants est supposée être l'initiateur) génère une paire de clés avec un des participants (feuilles) au groupe de diffusion groupée en utilisant une technique standard d'échange de clé publique (par exemple, un échange de clé publique Diffie-Hellman). La racine va ensuite fournir les paramètres d'association de sécurité de la diffusion groupée (qui peuvent être différents des paramètres de la paire de clés initiale) à cette première feuille. Les paramètres peuvent inclure des éléments tels que la classification et la politique. Une négociation (par l'usage du protocole de gestion d'association de sécurité (SAMP, *Security Association Management Protocol*) des paramètres peut être nécessaire. Il existe une possibilité que la feuille rejette la connexion au groupe de diffusion groupée sur la base des paramètres ci-dessus et de la liste du groupe de diffusion groupée. Si la feuille rejette cette session, la racine va répéter ce processus avec une autre feuille.

Une fois qu'une feuille a accepté de participer à la session de diffusion groupée, ces deux là choisissent ensuite une clé réseau à utiliser par le groupe de diffusion groupée. La clé réseau pourrait être générée au moyen d'un autre échange de clé publique entre les deux entités, ou simplement choisie par la racine, selon la politique qui est en place pour le groupe de diffusion groupée (c'est-à-dire que cette décision de politique ne sera pas un réel choix de temps). La question ici est le niveau de confiance que la feuille a envers la racine. Si l'échange initial de paire de clés assure un certain niveau d'authentification de l'utilisateur, il semble alors adéquat que seule la racine choisisse la clé réseau à ce stade. Une autre question est le niveau de confiance dans la force de la sécurité de la clé générée. Par un processus coopératif, les deux entités (la feuille et la racine) vont fournir des informations à utiliser dans la formation de la clé réseau.

La racine effectue alors un échange de paire de clés avec une autre feuille et effectue facultativement la négociation dont on a parlé précédemment. Lorsque la feuille accepte de se joindre au groupe de diffusion groupée, la racine envoie la clé réseau à la feuille.

Cet échange de paire de clés et la distribution de la clé réseau continuent pour tous les N usagers du groupe de diffusion groupée.

Racine et feuilles mettent en antémémoire la paire de clés pour les futures utilisations. Ces clés servent de clés de chiffrement de clé (KEK, *Key Encryption Key*) utilisées pour le changement des clés des feuilles ultérieurement sur le réseau. Seule la racine va mettre en antémémoire toutes les paires de clés des feuilles. Chaque feuille individuelle va mettre seulement en antémémoire sa propre paire unique de clés de chiffrement de clé.

Il y a deux cas à considérer lors de la mise en antémémoire des KEK. Le premier cas est lorsque la clé réseau et la KEK sont des clé pour la session. Dans ce cas, si on veut exclure un participant au groupe de la session de diffusion groupée (et remplacer la clé des participants restants par une nouvelle clé réseau) la racine va distribuer une nouvelle clé réseau chiffrée avec chaque KEK individuelle à chaque participant légitime restant. Ces KEK sont supprimées une fois que la session de diffusion groupée est achevée.

Le second cas à considérer est lorsque les KEK sont valides pour plus d'une session. Dans ce cas, la clé réseau peut aussi être valide pour plusieurs sessions, ou la clé réseau peut n'être encore valide que pour une session comme dans le cas ci-dessus. Que la clé réseau soit valide pour une session ou pour plus d'une session, la KEK sera mise en antémémoire. Si la clé réseau n'est valide que pour la session, les KEK seront utilisées pour chiffrer les nouvelles clés réseau pour les sessions de diffusion groupée suivantes. La suppression de participants au groupe survient comme dans le cas précédent décrit plus haut, sans considération de si la clé réseau est par session ou à utiliser sur plusieurs sessions.

Un schéma comme celui-ci peut être séduisant pour un usager parce que c'est une extension directe des techniques d'échange de clé publique certifiable. Il peut plaire aussi parce qu'il n'implique pas de tiers. Seuls les participants qui font

partie de la session de diffusion groupée participent au mécanisme des clés. Ce qui rend ce schéma aussi indésirable est qu'il va consommer intensivement de la transmission à mesure de la croissance en nombre, même pour les participants les plus efficaces en capacité de calcul, sans mentionner le cas de ceux dont les capacités en matériel sont moindres (tactique, sans fil, etc.). Chaque fois qu'apparaît le besoin d'éliminer un participant "non autorisé", une nouvelle clé réseau doit être distribuée.

Cette distribution exige une transmission de la racine à chaque participant restant, par laquelle la nouvelle clé réseau sera chiffrée avec la clé de chiffrement de clé (KEK) de paire unique de chaque participant.

Note: Cette approche est essentiellement la même que celle proposée au sous groupe de travail Sécurité de l'équipe d'ingénierie de l'Internet (IETF) [1], [2].

On notera aussi qu'il existe de nombreuses variantes d'une telle approche. Par exemple, au lieu que la racine fasse tous les N échanges de clé, la racine pourrait passer certaines de ces fonctionnalités (et du contrôle) à un certain nombre de feuilles en dessous d'elle. Par exemple, la liste du groupe de diffusion groupée pourrait être partagée en deux et la racine pourrait dire à une feuille de prendre la moitié des utilisateurs et d'effectuer l'échange de clés avec eux (puis de distribuer la clé réseau) tandis que la racine prendrait soin de l'autre moitié de la liste. (Les feuilles choisies fonctionneraient donc comme une racine et on peut les appeler des "sous-racines". Ces sous-racines auraient des feuilles en dessous d'elles, et les sous-racines entretiendraient la KEK de chaque feuille derrière elle). Cela s'adapte mieux que l'approche d'origine quand N devient grand. En particulier, cela exige moins de temps à établir le réseau de diffusion groupée (ou changer la clé) parce que la responsabilité particulière d'effectuer les échanges de paires de clé et de distribution de la clé réseau va être partagée entre plusieurs participants au groupe et peut être effectuée en parallèle, par opposition à la racine qui distribue seule la clé réseau à tous les participants.

Ce schéma n'est pas sans poser ses propres problèmes de sécurité. Il repousse la confiance à chaque contrôleur de sous-groupe – la racine suppose que ces contrôleurs de "sous-racine" agissent de façon digne de confiance. Chaque élément de contrôle (racine et sous-racine) doit rester dans le système tout au long de la diffusion groupée. Cela rend effectivement plus dur de retirer quelqu'un du réseau (en particulier les sous-racines) et plus lent du fait du contrôle réparti. Lorsque on retire un participant du groupe de diffusion groupée qui a fonctionné au nom de la racine, comme sous-racine, pour distribuer la clé réseau, des étapes supplémentaires seront nécessaires. Une nouvelle sous-racine doit être déléguée par la racine pour remplacer la sous-racine retirée. Un échange de clé (pour générer une nouvelle paire de KEK) doit se faire entre la nouvelle sous-racine et chaque feuille dont la sous-racine retirée était responsable. Une nouvelle clé réseau sera maintenant distribuée à partir de la racine aux sous-racines, et aux feuilles. Noter que cette dernière étape aurait été la seule étape requise si la partie retirée avait été une feuille sans responsabilité de contrôle.

5.3 Approche de la variable complémentaire

Supposons que nous avons N feuilles. La racine effectue un échange de clé publique avec chaque feuille i (i = 1, 2, ..., N). La racine va mettre en antémémoire chaque paire de KEK. Chaque feuille mémorise sa propre KEK. La racine va fournir la liste des participants au groupe de diffusion groupée et des attributs à tous les usagers. Les participants vont accepter ou rejeter leur participation à la session de diffusion groupée comme décrit dans les sections précédentes. La racine envoie à chaque feuille la clé réseau chiffrée pour le groupe de diffusion groupée en utilisant sa propre KEK(i) unique. (La racine a généré elle-même cette clé réseau, ou l'a générée en coopérant avec une des feuilles, comme on l'a expliqué précédemment). En plus de la clé réseau chiffrée, la racine va aussi chiffrer ce qu'on appelle des variables complémentaires et les envoyer aux feuilles.

Une feuille NE VA PAS recevoir sa propre variable complémentaire mais celle de la feuille N-1. La racine envoie la clé réseau et les variables complémentaires j, où j = 1, 2 ,..., N et j n'est pas égal à i, chiffrées par la KEK(i) à chaque feuille. Donc, chaque feuille reçoit et mémorise N variables qui sont la clé réseau, et N-1 variables complémentaires.

Donc, sortir un usager du groupe de diffusion groupée et reprendre les participants restants avec une nouvelle clé réseau va impliquer ce qui suit. Fondamentalement, pour couper la feuille n° 20 du réseau, un message est envoyé pour dire "couper la feuille 20 du réseau". Toutes les autres feuilles (et la racine) génèrent une nouvelle clé réseau sur la base de la clé réseau actuelle et de la variable complémentaire 20. (Donc, un certain type de processus de génération de variable de clé déterministe sera nécessaire pour tous les participants au groupe de diffusion groupée). Cette variable fraîchement générée va être utilisée comme nouvelle clé réseau par tous les participants restants au groupe de diffusion groupée. Tous, sauf la feuille 20 seront capables de générer la nouvelle clé réseau, parce qu'ils ont la variable complémentaire 20, mais pas la feuille 20.

Un schéma comme celui-ci semble très souhaitable du point de vue des économies de transmission car un message de changement de clé chiffré avec chaque KEK individuelle n'a pas à être envoyé à chaque feuille pour supprimer quelqu'un

du réseau. En d'autres termes, il y aura un message en clair au groupe de diffusion groupée contre N messages de changement de clé chiffrés. Il existe deux inconvénients majeurs à ce schéma. Le premier est l'exigence de capacités de mémorisation nécessaires pour les (N-1) variables complémentaires. Le second est que lorsque on supprime plusieurs usagers du groupe de diffusion groupée, le risque de collusion va poser problème. Ce que cela signifie est que les usagers supprimés pourraient travailler ensemble et partager leurs variables complémentaires individuelles pour retrouver l'accès à la session de diffusion groupée.

5.4 Approche de l'arborescence hiérarchique

L'approche de l'arborescence hiérarchique est celle que nous recommandons pour traiter le problème de la gestion des clés de diffusion groupée. Cette approche répond aux exigences de caractéristiques suivantes :

1. elle assure la suppression en toute sécurité du sein du groupe de diffusion groupée d'un utilisateur compromis,
2. elle assure l'efficacité de la transmission,
3. elle assure l'efficacité de la mémorisation.

Cette approche fait un équilibre entre le coût du temps, la mémorisation et le nombre de transmissions de message exigé, en utilisant un système hiérarchique de clés auxiliaires pour faciliter la distribution d'une nouvelle clé réseau. Il en résulte que l'exigence de mémorisation pour chaque utilisateur et que les transmissions requises pour le remplacement de clés sont toutes deux logarithmiques du nombre d'usagers, sans rapport avec les transmissions requises. Cette approche est robuste à l'égard de la collusion des utilisateurs exclus. De plus, alors que le schéma est hiérarchique par nature, aucune infrastructure n'est nécessaire au delà d'un serveur (par exemple, une racine) bien que la présence de tels éléments pourrait être avantageuse (voir la Figure 1).

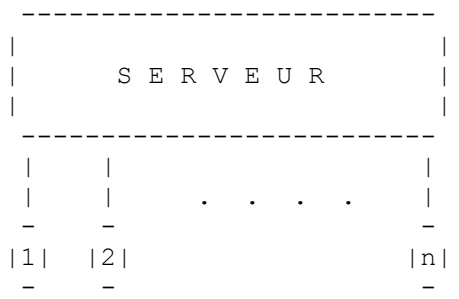

Figure 1 : Architecture de communication supposée

Les avantages et inconvénients du schéma sont énumérés plus en détails ci-dessous. Considérons la Figure 2. Elle illustre l'architecture logique de distribution des clés, où les clés n'existent qu'au serveur et chez les usagers. Donc, le serveur dans cette architecture va détenir les clés A à O, et les KEK de chaque usager. L'usager 11 dans cette architecture va détenir sa propre KEK unique, et les clés F, K, N, et O.

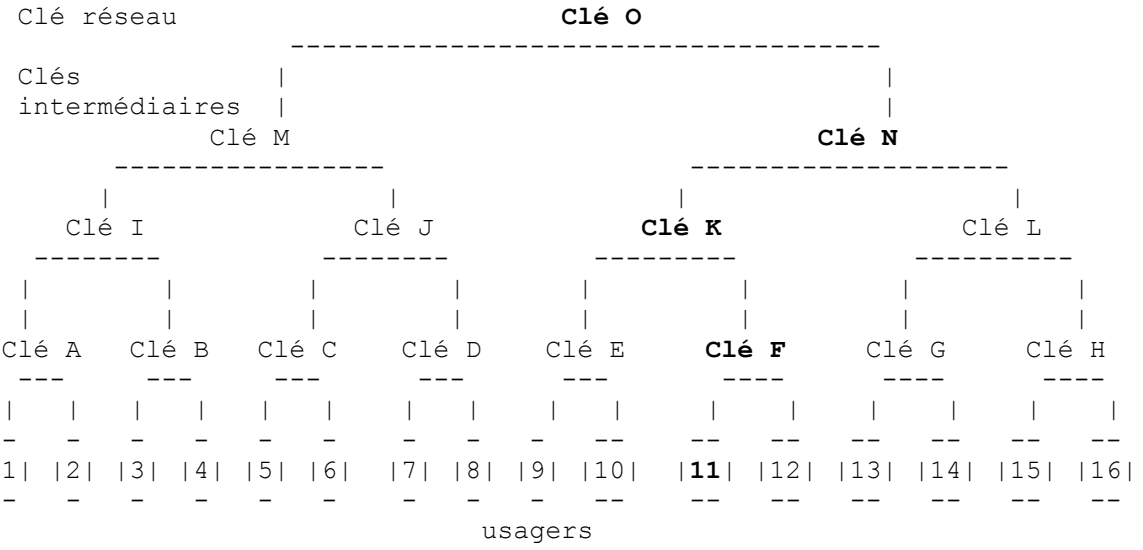

Figure 2 : Architecture logique de distribution de clés

On décrit maintenant l'organisation de la hiérarchie des clés et le processus d'établissement. La description va préciser

comment ajouter des usagers après la mise en place de la hiérarchie ; on va aussi décrire le retrait d'un usager. Noter que pour simplifier l'exposé, on n'a pas inclus le passage de la liste du groupe de diffusion groupée ni les protocoles de négociation.

On construit une arborescence avec racine (du bas vers le haut) où une feuille correspond à chaque usager, comme dans la Figure 2. (Bien qu'on ait dessiné un arbre binaire équilibré pour simplifier, il n'est pas nécessaire que l'arborescence soit équilibrée ou binaire – une analyse préliminaire de la forme de l'arborescence a été faite.) Chaque usager établit une paire de clés unique avec le serveur. Pour les usagers avec des capacités de transmission, cela peut être fait en utilisant le protocole d'échange de clé publique. La situation est plus compliquée pour les usagers en réception seule ; il est facile de supposer que ces usagers ont des clés pré-établies.

Une fois que chaque usager a une paire de clés connue du serveur, celui-ci génère (selon la politique de sécurité en place pour cette session) une clé pour chaque nœud restant dans l'arborescence. Les clés elles-mêmes devraient être générées par un processus robuste. On va aussi supposer que les usagers n'ont pas d'informations sur les clés dont ils n'ont pas besoin. (Noter qu'il n'y a pas d'utilisateur sur ces nœuds restants, c'est-à-dire que ce sont des nœuds logiques, et que la clé pour chaque nœud doit seulement être générée par le serveur via des moyens sûrs.) En commençant par les nœuds dont tous les enfants sont des feuilles et en progressant vers la racine, le serveur transmet la clé pour chaque nœud, chiffrée en utilisant les clés pour chacun des enfants de ce nœud. À la fin du procès, chaque usager peut déterminer les clés qui correspondent aux nœuds au-dessus de sa feuille. En particulier, tous les usagers détiennent la clé racine, qui va servir de clé réseau commune pour le groupe. L'exigence de capacité mémoire pour un usager à la profondeur d est d+1 clés. (Donc, pour l'exemple de la Figure 2, un usager à la profondeur d = 4 va détenir cinq clés. À savoir, la clé de chiffrement de clé unique générée par suite de l'échange de la paire de clés, trois clés de nœud intermédiaire – chacune chiffrée et transmise séparément, et la clé réseau commune pour le groupe de diffusion groupée qui est aussi chiffrée séparément.)

Il est aussi possible de transmettre toutes les clés de nœud intermédiaire et la clé du nœud racine en un seul message, où les clés de nœuds seraient toutes chiffrées avec la clé de paire unique de la feuille individuelle. De cette manière, une seule transmission (d'un plus gros message) est nécessaire par usager pour recevoir toutes les clés de nœuds (à comparer à d transmissions). On note que pour cette méthode, la feuille aura besoin d'un moyen pour déterminer quelle clé correspond à quel niveau de nœud.

Il est important de noter que cette approche requiert au serveur des capacités de traitement supplémentaires alors que peut-être d'autres approches ne l'exigent pas. Dans le pire des cas, un serveur sera chargé de générer les clés intermédiaires exigées par l'architecture.

5.4.1 Principe d'exclusion

Supposons que l'usager 11 (marqué en gras à la Figure 2) doive être supprimé du groupe de diffusion groupée. Alors, toutes les clés détenues par l'usager 11 (clés en gras F, K, N, O) doivent être changées et distribuées aux usagers qui en ont besoin, sans permettre à l'usager 11 ni à personne d'autre de les obtenir. Pour ce faire, on doit remplacer les clés en gras détenues par l'usager 11, en procédant de bas en haut. Le serveur choisit une nouvelle clé pour le nœud inférieur, puis la transmet chiffrée avec les clés filles appropriées. (Ces transmissions sont représentées par les lignes en pointillé). Donc pour cet exemple, la première clé remplacée est la clé F, et cette nouvelle clé sera envoyée chiffrée avec la clé de la paire unique de l'usager 12.

Comme on procède du bas vers le haut, chaque clé de remplacement aura été remplacée avant qu'elle ne soit utilisée pour chiffrer une autre clé. (Donc, pour le remplacement de la clé K, cette nouvelle clé sera envoyée chiffrée avec la clé fraîchement remplacée F (pour l'usager 12) et sera aussi envoyée comme transmission en diffusion groupée chiffrée ave la clé de nœud partagée par les usagers 9 et 10 (clé E). Pour le remplacement de la clé N, cette nouvelle clé sera envoyée chiffrée avec la clé K fraîchement remplacée (pour les usagers 9, 10, et 12) et sera aussi chiffrée avec la clé de nœud partagée par les usagers 13, 14, 15, et 16 (clé L). Pour le remplacement de la clé O, cette nouvelle clé sera envoyée chiffrée avec la clé N nouvellement remplacée (pour les usagers 9, 10, 12, 13, 14, 15, et 16) et sera aussi chiffrée avec la clé de nœud partagée par les usagers 1, 2 , 3, 4, 5, 6, 7, et 8 (clé M). Le nombre de transmissions requis est la somme des degrés des nœuds remplacés. Dans une arborescence à k niveaux dans lequel a se tient à la profondeur d, cela donne au plus kd-1 transmissions. Donc dans cet exemple, sept transmissions seront nécessaires pour exclure l'usager 11 du groupe de diffusion groupée et pour ramener les 15 autres usagers avec une nouvelle clé réseau de groupe de diffusion groupée à laquelle l'usager 11 n'a pas accès. Il est aisé de voir que le système est robuste contre la collusion, parce que aucun ensemble d'usagers ne peut lire de message si l'un d'eux a pu le lire individuellement.

Si la même stratégie que dans la section précédente est suivie pour envoyer plusieurs clés dans un message, le nombre de transmissions requises peut être réduit même jusqu'à quatre transmissions. Noter là encore que les messages seront plus gros en nombre de bits transmis. De plus, il doit exister un moyen pour chaque feuille de déterminer quelle clé dans le message correspond à quel nœud de la hiérarchie. Donc, dans cet exemple, pour le remplacement des clés F, K, N, et O

pour l'usager 12, les quatre clés seront chiffrées dans un message avec la clé de la paire unique de l'usager 12. Pour remplacer les clés K, N, et O pour les usagers 9 et 10, les trois clés seront chiffrées dans un message avec la clé de nœud partagée par les usagers 9 et 10 (clé E). Pour remplacer les clés N et O pour les usagers 13, 14, 15, 16, les deux clés seront chiffrées dans un message sous la clé de nœud partagée par les usagers 13, 14, 15, et 16 (clé L). Finalement, pour remplacer la clé O pour les usagers 1, 2 , 3, 4, 5, 6, 7, et 8, la clé O sera chiffrée sous la clé de nœud partagée par les usagers 1, 2 , 3, 4, 5, 6, 7, et 8 (clé M). Donc, le nombre de transmission requis est au plus de (k-1)d.

Le tableau suivant montre la suppression d'un usager, et comment les exigences de mémorisation et de transmission augmentent avec le nombre d'usagers.

Tableau 1 : Coût de mémorisation et de transmission

Nombre d'utilisateurs (k)	Degré	Mémorisation par usager (d+1)	Transmissions pour changer les clés des participants restants du groupe de diffusion groupée, une clé par message (kd-1)	Transmissions pour changer les clés des participants restants du groupe de diffusion groupée, plusieurs clés par message (k-1)d
8	2	4	5	3
9	3	3	5	4
16	2	5	7	4
2 048	2	12	21	11
2 187	3	8	20	14
131 072	2	18	33	17
177 147	3	12	32	22

Les avantages d'un tel schéma sont :

1. Les coûts de mémorisation chez l'usager et de transmissions de changement de clés sont équilibrés et s'adaptent à la croissance du nombre d'usagers. Ce n'est pas le cas pour [1], [2], ou [4].

2. Les clés auxiliaires peuvent être utilisées pour transmettre non seulement d'autres clés, mais aussi des messages. Donc, la hiérarchie peut être conçue pour mettre en place des sous-groupes qui souhaitent communiquer en toute sécurité (c'est-à-dire, sans transmettre au reste du grand groupe de diffusion groupée) entre certains nœuds, éliminant le besoin d'une maintenance de clés réseau séparée pour ces sous-groupes. Cela fonctionne le mieux si les utilisateurs opèrent dans une hiérarchie pour commencer (par exemple, des opérations militaires) qui peuvent être reflétées par la hiérarchie des clés.

3. La hiérarchie peut être conçue pour refléter l'architecture du réseau, augmentant l'efficacité (chaque usager reçoit moins de messages qui ne le concernent pas). Aussi, les responsabilités du serveur peuvent être partagées entre les sous-racines (toutes doivent être sécurisées).

4. Le risque pour la sécurité associé aux usagers en réception seule peut être minimisé en rassemblant ces usagers dans une zone particulière de l'arborescence.

5. Cette approche est résistante à la collusion entre un nombre arbitraire d'usagers.

Comme on l'a déjà noté, dans le procès de changement de clé après la compromission d'un usager, dans le cas d'une clé par message, chaque clé remplacée doit être déchiffrée avec succès avant que la prochaine clé puisse être remplacée (sauf si les usagers peuvent mettre en antémémoire les messages de changement de clé). Ce goulet d'étranglement peut être un problème sur un réseau bruyant ou lent. (Si plusieurs usagers sont retirés, cela peut être mis en parallèle, de sorte que le temps nécessaire au changement de clés est en gros indépendant du nombre d'usagers retirés.)

En augmentant les valences et en diminuant la profondeur de l'arbre, on peut réduire les exigences de mémorisation pour les usagers, au prix d'une augmentation des transmissions. Par exemple, dans le cas d'une clé par message, si n usagers sont répartis dans un arbre à k niveaux, chaque usager aura besoin de capacités de mémorisation. Le changement de clé après le retrait d'un usager exige maintenant des transmissions. Lorsque k tend vers n, cela s'approche du schéma de paire de clés décrit précédemment dans cet article.

5.4.2 Options de l'approche de l'arborescence hiérarchisée

5.4.2.1 Approche de l'arborescence hiérarchisée répartie

L'approche de l'arborescence hiérarchisée présentée dans cette section pourrait être répartie comme indiqué au paragraphe 5.2 pour ressembler de plus près à la proposition avancée dans [4]. Des sous-racines peuvent exister à chacun des nœuds pour traiter toute adjonction ou changement de clé qui serait nécessaire pour un des usagers subordonnés. Cela pourrait être particulièrement intéressant pour les usagers qui n'ont pas de connexion directe avec la racine. On rappelle, comme indiqué au paragraphe 5.2, que la confiance placée dans ces sous-racines pour agir avec l'autorité et la sécurité d'une racine est une proposition potentiellement dangereuse. On trouvera un écho à cette idée dans [4].

Voici quelques recommandations pratiques qui pourraient être faites pour ces sous-racines. Il ne devrait pas être permis aux sous-racines de changer la liste des participants au groupe de diffusion groupée qui leur a été fournie par la racine. Une méthode pour ce faire serait que la racine signe la liste avant de la fournir aux sous-racines. Les sous-racines autorisées pourraient cependant être autorisées à établir de nouveaux groupes de diffusion groupée pour les usagers en dessous d'eux dans la hiérarchie.

Il est important de noter que bien que cette distribution puisse paraître fournir des avantages en terme de temps requis pour initialiser le groupe de diffusion groupée (comparé au temps requis pour initialiser le groupe décrit au paragraphe 5.4) et pour les changements de clé périodiques, elle ne paraît fournir aucun avantage pour changer les clés du groupe de diffusion groupée lorsque un usager a été compromis.

On note aussi que quel que soit le schéma de gestion de clé (arborescence hiérarchisée, arborescence hiérarchisée répartie, arborescence fondée sur un cœur , GKMP [2], etc.) il faudra subir une "touche" pour initialiser le groupe de diffusion groupée avec la première clé réseau du groupe de diffusion groupée. Donc, l'approche de l'arborescence hiérarchisée ne souffre pas de la complexité supplémentaire comparée aux autres schémas par rapport à l'initialisation.

5.4.2.2 Formation de groupe de diffusion groupée

Bien que cet article ait présenté la formation du groupe de diffusion groupée comme étant à l'initiative de la racine, l'approche hiérarchique est cohérente avec l'adhésion à l'initiative de l'usager. Celle-ci est la méthode de formation de groupe de diffusion groupée présentée dans [4]. L'adhésion à l'initiative de l'usager peut être souhaitable lorsque un sous-ensemble central d'usagers au sein du groupe de diffusion groupée a besoin d'être mis en ligne et de communiquer plus rapidement. Les autres participants au groupe de diffusion groupée peuvent alors être mis en ligne lorsque ils le souhaitent. Cependant, dans ce type d'approche, il n'existe pas une limite de temps définie au bout de laquelle on peut être sûr que tous les participants feront partie du groupe de diffusion groupée.

Par exemple, dans le cas d'une seule racine, la hiérarchie est établie une seule fois, au début, par l'initiateur (qui est habituellement aussi la racine) qui génère aussi la liste des participants au groupe. Le groupe de clés pour chaque participant peut être alors demandé individuellement (tiré) aussitôt (mais pas avant) qu'un participant souhaite se joindre à la session.

5.4.2.3 Authentification spécifique de l'envoyeur

Dans l'environnement de diffusion groupée, il existe la possibilité que les participants au groupe veuillent parfois identifier de façon univoque quel participant est l'envoyeur d'un message au groupe de diffusion groupée. Dans le système de distribution de clé de diffusion groupée décrit par Ballardie [4], la notion de "clés spécifiques de l'envoyeur" est présentée.

Une autre option pour permettre aux participants d'un groupe de diffusion groupée de déterminer de façon univoque l'envoyeur d'un message est par l'utilisation d'un processus de signature. Lorsque un membre du groupe de diffusion groupée signe un message avec sa propre clé de signature privée, le receveur de ce message signé dans le groupe de diffusion groupée peut utiliser la clé de vérification publique de l'envoyeur pour déterminer si le message est de qui il prétend être.

Une autre idée qui se rapporte à cela est le cas où deux usagers d'un groupe de diffusion groupée veulent communiquer strictement l'un avec l'autre, et veulent que personne d'autre n'écoute la communication. Si cette relation de communication est connue lors de l'établissement original du groupe de diffusion groupée, ces deux participants pourraient simplement être placés adjacents l'un à l'autre au plus bas niveau de la hiérarchie (en dessous d'un nœud binaire). Donc, ils vont naturellement partager une paire de clés secrètes. Autrement, une façon simple de réaliser cela est d'effectuer un échange de paire de clés fondé sur une clé publique entre les deux utilisateurs pour générer une clé de chiffrement de trafic pour leurs communications privées en envoi individuel. Par ce processus, non seulement les transmissions chiffrées entre eux ne seront lisibles que par eux, mais l'authentification univoque de l'envoyeur peut être réalisée via l'échange de paire fondé sur la clé publique.

5.4.2.4 Changement de clés de groupe de diffusion groupée et utilisation de KEK de groupe

La référence [4] utilise une clé de chiffrement de clé de groupe qui peut être partagée par le groupe de diffusion groupée pour l'utiliser dans les changements de clé périodiques du groupe de diffusion groupée. Sans parler des inconvénients potentiels pour la sécurité de la mise en œuvre d'une clé partagée pour le chiffrement de clés futures, l'utilisation d'une clé de chiffrement de clé de groupe est sans intérêt pour un groupe de diffusion groupée si un changement de clé est nécessaire du fait de la compromission connue de l'un des membres. La stratégie pour changer les clés du groupe de diffusion groupée présentée au paragraphe 5.4.1 traite précisément de ce problème critique et offre un moyen de réaliser cette tâche avec des exigences minimales de transmission et de mémorisation de message.

On peut cependant se poser la question de savoir si le changement de clés d'un groupe de diffusion groupée sera nécessaire dans un scénario de non compromission. Par exemple, si un usager décide qu'il ne veut plus participer au groupe, et demande au contrôleur de liste de le retirer de la liste des participants au groupe de diffusion groupée, un changement des clés du groupe de diffusion groupée sera t-il nécessaire ? Si la politique de sécurité du groupe de diffusion groupée rend obligatoire que les usagers supprimés ne puissent plus recevoir les transmissions, alors un changement de la clé réseau sera nécessaire. Si la politique de sécurité du groupe de diffusion groupée ne se soucie pas que les personnes supprimées puissent encore déchiffrer les transmissions (chiffrées avec la clé réseau du groupe qu'elles pourraient encore détenir) mais tient à ce qu'elles ne puissent pas chiffrer et transmettre de messages, un changement de clé sera là encore nécessaire. La seule solution de remplacement au changement de clé du groupe de diffusion groupée dans ce scénario exigerait d'un receveur qu'il vérifie chaque envoyeur de message reçu, par rapport à la liste des participants du groupe. Et donc de rejeter tout message envoyé par un usager qui n'est pas sur la liste. Ceci n'est pas une option praticable. Donc, il est recommandé de toujours changer les clés du groupe de diffusion groupée lorsque quelqu'un est supprimé, que ce soit pour des raisons de compromission ou non.

5.4.2.5 Retrait en gros de participants

Comme indiqué à la Section 2, le besoin peut se faire sentir de retirer en bloc des usagers. Si les usagers sont répartis comme exposé au paragraphe 5.4.1 en sous-groupes qui souhaitent communiquer en toute sécurité en étant tous sous le même nœud, la suppression en bloc des usagers peut être faite assez simplement si tout le nœud est à supprimer. On utilise la même technique que décrite au paragraphe 5.4.1 pour changer les clés de toute clé de nœud partagée que détiennent les participants restants en commun avec le nœud retiré.

Le problème du retrait en bloc devient plus difficile lorsque les participants à retirer sont dispersés dans toute l'arborescence. Selon le nombre de participants à retirer, et l'endroit où ils sont situés dans la hiérarchie, le nombre de transmissions requis pour changer les clés du groupe de diffusion groupée peut être équivalent à un changement de clé brutal des participants restants. La question peut aussi être soulevée de savoir jusqu'à quel point les usagers restants sont restructurés dans une nouvelle arborescence hiérarchisée, ou si un nouveau groupe de diffusion groupée devrait être formé. Restructurer l'arborescence hiérarchisée devrait probablement être l'option préférée, parce qu'elle ne va pas nécessiter d'effectuer à nouveau les échanges de paires de clés pour former les nouvelles KEK uniques d'usager.

5.4.2.6 Compatibilité ISAKMP

Jusqu'à présent, ce document s'est principalement concentré sur les compromis architecturaux impliqués par la génération, distribution, et maintenance des clés de chiffrement de trafic (clés réseau) pour les groupes de diffusion groupée. D'autres éléments sont impliqués dans l'établissement d'une connexion sûre entre les participants à une diffusion groupé, qui n'ont pas été discutés en détail. Par exemple, le concept d'être capable de "faire un choix" et de négocier les capacités du mécanisme d'échange de clés et de divers autres éléments est un aspect très important et nécessaire.

La proposition de la NSA au sous groupe de travail Sécurité de l'équipe d'ingénierie de l'Internet (IETF) [3] intitulé "Association de sécurité Internet et protocole de gestion de clés (ISAKMP)" a tenté d'identifier les divers éléments fonctionnels requis pour l'établissement d'une connexion sûre pour le plus grand réseau actuel, l'Internet. Bien que la proposition se concentre actuellement sur le problème des connexions point à point, les éléments fonctionnels devraient être les mêmes pour les connexions de diffusion groupée, avec les changements appropriés aux techniques choisies pour mettre en œuvre les éléments fonctionnels individuels. Donc, la mise en œuvre de ISAKMP est compatible avec l'utilisation de l'approche de l'arborescence hiérarchisée.

6. Résumé

Comme on l'expose dans ce rapport, il y a deux principaux domaines qui posent problème lorsque on cherche des solutions au problème de la gestion des clés de diffusion groupée. Ce sont l'initialisation sûre et le changement de clés du groupe de

diffusion groupée avec une clé réseau commune. À présent, plusieurs articles traitent de l'initialisation d'un groupe de diffusion groupée, mais ils ne traitent pas de façon satisfaisante comment supprimer efficacement et de façon sûre un usager compromis du groupe de diffusion groupée.

Le présent article propose une approche d'arborescence hiérarchisée pour résoudre ce problème difficile. Elle est robuste contre la collusion, tout en équilibrant en même temps le nombre de transmissions et la mémorisations exigés pour changer les clés du groupe de diffusion groupée en cas de compromission.

Il est aussi important de noter que la proposition recommandée dans cet article est cohérente avec les autres solutions de gestion de clé de diffusion groupée [4], et qu'elle permet de nombreuses options pour sa mise en œuvre.

7. Considérations pour la sécurité

Les questions de sécurité sont discutées tout au long de ce mémoire.

8. Références

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

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

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

[4] A. Ballardie, "Distribution de clés en diffusion groupé échelonnable", RFC1949, mai 1996. *(Expérimentale)*

[5] Wong, C., Gouda, M. and S. Lam, "Secure Group Communications Using Key Graphs", Technical Report TR 97-23, Department of Computer Sciences, The University of Texas at Austin, juillet 1997.

Adresse des auteurs

Debby M. Wallner
National Security Agency
Attn: R2
9800 Savage Road STE 6451
Ft. Meade, MD. 20755-6451
téléphone : 301-688-0331
mél : dmwalln@orion.ncsc.mil

Eric J. Harder
National Security Agency
Attn: R2
9800 Savage Road STE 6451
Ft. Meade, MD. 20755-6451
téléphone : 301-688-0850
mél : ejh@tycho.ncsc.mil

Ryan C. Agee
National Security Agency
Attn: R2
9800 Savage Road STE 6451
Ft. Meade, MD. 20755-6451

Déclaration de droits de reproduction

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