Groupe de travail Réseau
Request for Comments : 2094
Catégorie : Expérimentale
Traduction Claude Brière de L'Isle

H. Harney
C. Muckenhirn
SPARTA, Inc.

juillet 1997

Architecture du protocole de gestion de clés de groupe (GKMP)

Statut de ce mémoire

Le présent mémoire définit un protocole expérimental pour la communauté de l'Internet. Il ne spécifie en aucune façon une norme de l'Internet. On invite à des discussions et suggestions pour son amélioration. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

La présente spécification propose un protocole pour créer des groupes de clé symétriques et les distribuer parmi les homologues en communication. Ce protocole présente les avantages d'être virtuellement invisible à l'opérateur, de ne pas avoir besoin d'un site central de distribution de clés, de ne donner les clés qu'aux membres du groupe, de fonctionner en mode envoyeur ou receveur, et de pouvoir faire usage des protocoles de communications de diffusion groupée.

Table des matières

1. Introduction

Le présent document décrit une architecture pour la gestion des clés cryptographiques pour les communications en diffusion groupée. On identifie les rôles et les responsabilités des éléments d'un système de communications en accomplissant la gestion des clés de diffusion groupée, on définit les exigences de sécurité et les exigences fonctionnelles de chacun, et on fournit une introduction détaillée au protocole de gestion de clés de groupe (GKMP, *Group Key Management Protocol*) qui donne la capacité de créer et distribuer les clés au sein de groupes de taille arbitraire sans l'intervention d'un gestionnaire de clés global/centralisé. Le GKMP combine les techniques développées pour la création de paires de clés avec les techniques utilisées pour distribuer les clés à partir d'un KDC (c'est-à-dire, le chiffrement symétrique des clés) pour distribuer les clés symétriques à un groupe d'hôtes.

1.1 Environnements de communications en diffusion groupée

Le travail qui a conduit à ce rapport était d'abord centré sur une commande et un contrôle militaire et des systèmes de contrôle d'armes, ces systèmes ont tendance à avoir des flux de communication descendants, de commandant à commandé. Le choix des parties qui vont être membres d'une communication particulière (par exemple, un groupe de diffusion groupée) est à la discrétion de la ou des parties de niveau "supérieur". Ce modèle "à l'initiative de l'envoyeur" (en supposant

que la partie de niveau supérieur envoie) se transpose bien en diffusion (comme dans l'électromagnétisme, l'espace, les transmissions) et les moyens de communications par circuit commuté (par exemple, la visioconférence, la diffusion groupée ATM).

En cherchant à appliquer cette technologie à l'Internet, il est apparu que c'est un modèle assez différent qui s'applique (au moins pour certaines portions du trafic de diffusion groupée de l'Internet). IDRP et le protocole d'acheminement de diffusion groupée par vecteur de distance (DVMRP, *Distance Vector Multicast Routing Protocol*) utilisent la diffusion groupée comme un mécanisme pour que les parties relaient des informations communes à leurs homologues. Chaque partie envoie et reçoit des informations sur le canal de diffusion groupée. Selon ce qui est approprié, une partie peut choisir de quitter ou de se joindre à la communication sans permission expresse d'une des autres parties (cela pose la question des méta autorisations qui permettent aux parties de coopérer). Plus intéressant, dans le modèle de diffusion groupée IP, le receveur dit au réseau de l'ajouter à la distribution pour une adresse de diffusion groupée particulière, qu'elle existe déjà ou non, et l'émetteur n'est pas consulté sur l'ajout du receveur.

D'autres applications des communications de diffusion groupée dans l'Internet, par exemple les diffusions NASA Select, peuvent être vues comme la mise en œuvre du modèle de l'envoyeur, car l'envoyeur choisit l'heure de la diffusion, le canal, et le contenu, mais pas les destinations.

Notre intention est de décrire les services de gestion de clés qui prennent en charge les modèles de communications (et le contrôle d'accès qu'ils impliquent) et fonctionnent aussi bien dans les environnements de commutation de circuit que de commutation de paquets.

1.2 Sécurité pour les diffusions groupées

Les communications en diffusion groupée, comme avec l'envoi individuel, peuvent exiger l'un des services de sécurité définis dans la norme ISO 7498, le contrôle d'accès, la confidentialité des données, la confidentialité du trafic, l'intégrité/authentification des données, l'authentification de la source, la non répudiation de l'envoyeur et du receveur, et l'assurance de service. Du point de vue des processus de gestion de clés, seules la confidentialité des données, l'authentification des données, et l'authentification de la source peuvent être prises en charge. Les autres services, confidentialité du trafic, non répudiation, et assurance du service doivent être fournis par le protocole de communications, ils peuvent s'appuyer sur des services cryptographiques mais ne sont pas garantis par eux.

2. Architectures de gestion de clé de diffusion groupée

2.1 Fonctionnement actuel

Il y a plusieurs mécanismes électroniques pour générer et distribuer des clés symétriques à plusieurs ordinateurs (c'est-à-dire, à des groupes de communications). Ces techniques s'appuient généralement sur un centre de distribution de clés (KDC, *Key Distribution Center*) pour agir comme intermédiaire de l'établissement des groupes de clés symétriques. Les systèmes militaires, comme BLACKER, STU-II/BELLFIELD, et EKMS, et les systèmes commerciaux, comme X9.17 et Kerberos, fonctionnent tous avec des KDC dédiés. Une demande de clé de groupe est envoyée au KDC via divers moyens (en ligne ou hors ligne). Le KDC agissant comme contrôleur d'accès décide si la demande est appropriée ou non (c'est-à-dire, tous les membres d'un groupe sont retenus pour recevoir toutes les données sur un groupe). Le KDC va alors appeler chaque membre individuel du groupe et télécharger la clé symétrique. Lorsque chaque membre a la clé, le KDC va le notifier au demandeur. Une communication de groupe sûre peut alors commencer. Bien que cela soit certainement plus rapide que tout ce qui exige une intervention humaine, cela exige quand même un certain délai d'établissement. Cependant, un tiers, dont le principal intérêt n'est pas la communication, doit être impliqué.

Des paires de clés peuvent être créées de façon autonome par l'hôte sur un réseau en utilisant un nombre quelconque de protocoles de génération de clés (FireFly, Diffe-Hellman, RSA). Ces protocoles s'appuient tous sur des algorithmes coopératifs de génération de clés pour créer une clé de chiffrement. Ces algorithmes s'appuient sur des informations aléatoires générées par chaque hôte. Ces algorithmes s'appuient aussi sur la vérification des permissions par l'homologue pour s'assurer que les partenaires à la communication sont bien ce qu'ils prétendent être et qu'ils ont l'autorisation de recevoir les informations qui sont transmises. Ce processus de révision par les homologues s'appuie sur une autorité de confiance qui alloue les permissions à chaque hôte qui, dans le réseau, veut la capacité de créer ces clés. La réelle beauté de ces protocoles de gestion de paires de clés est qu'ils peuvent être intégrés dans le protocole de communication ou dans l'application. Cela signifie que la gestion de clés devient relativement invisible aux personnes dans le système.

2.2 Fonctionnements fondés sur GKMP

Le GKMP décrit ci-dessous, délègue le contrôle d'accès, la génération des clés, et les fonctions de distribution aux entités communicantes elles-mêmes plutôt que de s'appuyer sur un tiers (le KDC) pour ces fonctions. En prélude à la distribution réelle des clés, on doit faire quelques hypothèses (pour les besoins du présent document) : il existe un "gestionnaire de la sécurité" responsable de la création et de la distribution aux parties des informations authentiques d'identification et des permissions de sécurité. La fonction de gestionnaire de la sécurité peut être réalisée à travers un système strictement hiérarchisé (STU-III) ou par un système ad hoc de "gestionnaires de domaine" 'homologues coopérant. La mise en œuvre de la hiérarchie de certification n'est pas traitée dans le présent document. Les parties communicantes sont en ligne pour les clés formées et distribuées par le GKMP.

2.2.1 Opérations à l'initiative de l'envoyeur

Ce paragraphe décrit le concept de base du fonctionnement de la gestion de clés de diffusion groupée pour la prise en charge de la diffusion groupée à l'initiative de l'envoyeur. Ce modèle de communications en diffusion groupée a été à la base de notre travail d'origine sur la gestion de clé de diffusion groupée. Du point de vue de la sécurité, l'application envoyeuse est capable de contrôler l'accès sur la transmission à la fois par la distribution des clés et par la distribution des communications (en n'envoyant pas la transmission à certaines adresses).

Identification du contrôleur de clé de groupe
L'origine du groupe de diffusion groupée crée ou obtient un certificat de gestion de groupe de sa hiérarchie de certification. Le certificat identifie le détenteur comme responsable de la génération et la distribution de la clé de groupe (les normes de dénomination ne sont pas visées ici, le nom devrait refléter les structures de désignation appropriées pour le service cryptographique pris en charge. Par exemple, les chiffreurs de niveau IP devraient utiliser des désignations qui reflètent les identités des "hôtes" (adresses IP, ou noms d'hôtes du DNS, un chiffreur RTP utilisera des noms de session). L'origine du groupe relaie la liste des membres à l'application de gestion de clé de groupe (GKM, *Group Key Management*).

Création de clé de groupe
L'application GKM, fonctionnant au nom de l'origine, choisit un membre du groupe, le contacte, et crée un paquet de clé de groupe (GKP, *Group Key Packet*). Un GKP contient la clé de chiffrement du trafic de groupe (GTEK, *group traffic encrypting key*) actuelle et la clé de chiffrement de clé de groupe (GKEK, *group key encrypting key*) future. L'application GKM s'identifie alors comme contrôleur de clé de groupe, ce que le membre valide, sous couvert du GTEK.

(GKP) = [GTEKn,GKEKn+1]

Au titre de la formation du paquet de clé de groupe sont choisis les paramètres d'usage, appropriés pour le système de chiffrement sous-jacent. À la différence de la négociation normale des paramètres, où arrivent le niveau et la gamme de sécurité communs et les services, l'application GKM de l'origine choisit ces paramètres et le membre doit s'y conformer.

Distribution de clé de groupe
Après la création du GKP, le contrôleur de groupe contacte chaque membre du groupe, crée un paquetage de clé de session (SKP, *Session Key Package*) valide leurs permissions (vérifie le certificat du membre par rapport aux paramètres du groupe) et crée un paquetage de changement de clé de groupe (GRP, *Group Rekey Package*) pour ce membre. Un SKP contient une TEK de session et une KEK de session pour un membre particulier. Un GRP contient le GKP chiffré dans une KEK et signé en utilisant le certificat de l'origine.

(SKP) = [STEK, SKEK]
(GRP) = {[GKP]KEK} SignatureController

Changement de clé de groupe
Lorsque le groupe a besoin de changer ses clés, l'application GKM d'origine choisit un membre, crée un nouveau GKP, crée un nouveau GRP (qui est chiffré dans la prochaine GKEK précédemment distribuée) et le diffuse au groupe.

Cette procédure est assez complexe, mais à part pour la distribution de certificats spécifiques du site, aucune ressource de gestion de clé centralisée n'est nécessaire. Les seules parties aux communications de la gestion de clés sont les mêmes que celles qui vont participer au groupe.

2.2.2 Opérations à l'initiative du receveur

Ce paragraphe décrit le concept du fonctionnement de la gestion de clé pour la prise en charge des communications de diffusion groupée à l'initiative du receveur. Le modèle à l'initiative du receveur présente des problèmes intéressants du point de vue de la sécurité car les participants finaux ne sont pas connus a priori. Et aussi, dans une application purement à

l'initiative du receveur (comme DVMRP) il n'y a pas de concept d'une "origine" et les participants au groupe peuvent être assez dynamiques, les participants changeant d'une minute à l'autre.

Pour que des communications de groupe sûres aient lieu, tous les membres doivent obtenir la même clé. Cela peut se faire soit en utilisant une technique déterministe de génération de clé (en utilisant un germe secret partagé) soit en rendant un membre du groupe responsable de la création de la clé. L'utilisation d'un générateur déterministe de clé pose des problèmes de sécurité, en particulier en ce qui concerne la perte du germe (cela compromet le trafic à la fois passé et futur). La désignation d'un membre pour le rôle de "contrôleur" de clé présente aussi des inconvénients, mais ceux-ci se rapportent à la détermination de qui devrait être le contrôleur et au besoin que chaque membre le contacte. Le reste de cet exposé va examiner comment le concept de "contrôleur" qu'on vient d'évoque pourrait fonctionner dans le cas à l'initiative du receveur.

Sélection du contrôleur de clé de groupe
Un membre du groupe va être chargé de l'établissement initial du groupe et de la génération périodique et de la dissémination des nouveaux GRP. Il n'est pas nécessaire que le contrôleur choisi le soit pour toujours, mais à tout moment, un seul contrôleur peut être actif pour chaque groupe. Le choix d'un contrôleur peut être fait par un système de vote, par défaut (le premier qui transmet au groupe est le contrôleur) ou par configuration.

L'identité actuelle du contrôleur doit être mise à la disposition de tous les membres, et des membres potentiels, pour le chargement initial de la clé de groupe et la récupération des erreurs. Les informations peuvent être relayées par diffusion sur un "canal" de gestion de clé, ou par un service de répertoire.

Création de clé de groupe
Le GKP est créé et distribué de la même façon que dans les opérations à l'initiative de l'envoyeur. Le contrôleur crée un GKP avec le premier membre du groupe qui initie le contact. L'application GKM s'identifie alors comme contrôleur de clé de groupe, ce que valide le membre, sous couvert de la GTEK. La négociation des paramètres est effectuée et le premier membre du groupe a sa clé.

Distribution de clé de groupe
Après la création du GKP, comme les autres membres contactent le contrôleur, une SKP est créée, les permissions des membres sont validées et un GRP est chargé par le membre.

Pour les groupes largement répartis, une forme de dissémination distribuée peut être utilisée. Un certain nombre d'applications GKM régionales sont activées avec la capacité de valider les permissions des nouveaux membres et si la validation réussit elles leur envoient le GKP en cours. (Le contrôle d'accès n'est pas défini dans le présent document, mais on suppose qu'aussi bien le contrôle d'accès hiérarchique que discrétionnaire (fondé sur une règle et fondé sur l'identité) seront pris en charge.) Ces distributeurs de clés régionaux effectuent les mêmes fonctions que le contrôleur, sauf qu'ils ne créent pas le GKP. Ce concept peut être étendu au point que tous les membres actuels soient capables de télécharger le GKP, et de passer cette capacité.

Changement de clé de groupe
Lorsque le groupe a besoin de changer les clés, la procédure sera identique au cas à l'initiative de l'envoyeur. L'application GKM qui contrôle choisit un membre, crée un nouveau GKP, crée un nouveau GRP (qui est chiffré dans la prochaine GKEK précédemment distribuée) et le diffuse au groupe.

2.3 Caractéristiques de GKMP

Ce paragraphe souligne les domaines dans lesquels on pense que l'approche de GKMP présente des avantages sur les approches "traditionnelles" fondées sur le KDC.

2.3.1 Diffusion groupée

Les protocoles de diffusion groupée sont un domaine d'intérêt croissant pour l'Internet. Le plus grand bénéfice d'un protocole de diffusion groupée est la capacité qu'ont plusieurs receveurs d'obtenir simultanément la même transmission. Si la transmission est de nature sensible, elle devrait être chiffrée. Cela signifie que tous les membres du groupe doivent partager la même clé de chiffrement pour tirer parti de la transmission en diffusion groupée.

Aujourd'hui, la seule façon d'établir un groupe de clés symétriques est avec l'assistance d'une facilité centralisée de gestion de clés. Cette facilité agirait comme un courtier en clés qui crée une clé de distribution pour qualifier les membres du groupe. Ce concept centralisé pose plusieurs problèmes. Ces problèmes sont à la source de nombre des motifs qui ont conduit à créer un protocole de gestion répartie des clés.

2.3.2 Augmentation de l'autonomie des groupes de clés

GKMP propose d'étendre le paradigme de la paire de clés aux clés de groupe. Ce protocole peut être intégré dans les protocoles ou applications de communication et peut devenir invisible à l'opérateur de l'hôte. On utilisera la révision par l'homologue pour mettre en application notre politique de sécurité.

GKMP permet à tout hôte d'un réseau de créer et gérer un groupe sûr. La maintenance de ces clés de groupe peut être effectuée par les hôtes intéressés dans le groupe. Les groupes eux-mêmes seront relativement autonomes. Cela simplifie l'installation de cette technologie, permettant que plus d'hôtes utilisent des communications de diffusion groupée sécurisées.

2.3.3 Latence

La latence se réfère au temps d'établissement ou de suppression du de changement de clé d'un groupe. En bref, cela correspond au temps que cela prendrait pour établir une adresse de diffusion groupée.

Le protocole GKMP peut permettre la délégation de l'autorité de création de groupe à tout hôte du réseau. Par nature, lorsque un hôte a besoin d'un groupe, il va avoir les outils nécessaires pour créer ce groupe et le gérer. De plus, comme l'hôte a simplement besoin de créer un seul groupe, il peut se concentrer sur ce groupe particulier.

Dans l'approche centralisée actuelle de distribution des clés, le groupe doit être demandé au site central. Le site central va traiter cette demande conformément à ses priorités et sa charge de travail. Une latence va se développer si la charge de travail du site central échappe à tout contrôle ou si les communications vers le site sont en surcharge.

2.3.4 Possibilité d'extension

Un des problèmes du système centralisé de distribution de clés est la concentration de la charge de travail de gestion des clés sur un seul site. Le processus de création des groupes de clés – création de clés, revue des accès, communication aux membres du groupe, consomme du temps et des efforts. Lorsque croît le nombre de groupes sur le réseau ainsi que le nombre de membres de groupe par groupe, la charge de travail au site central atteint rapidement les limites de la capacité.

GKMP devrait permettre à un grand nombre de groupes d'exister sur l'Internet sans surcharge d'un hôte particulier. La délégation de la charge de la création et de la gestion à l'échelle de la Toile fait passer le fardeau de la maintenance des groupes au hôtes intéressés à l'utilisation de ces groupes. C'est non seulement plus efficace mais cela place la charge à l'endroit approprié.

Le protocole GKMP distribue à travers les réseaux les exigences de communication pour la gestion des groupes. Chaque groupe gère le groupe en utilisant les mêmes ressources de communication nécessaires pour écouler le trafic. Il est vraisemblable que si un groupe de communication peut prendre en charge le trafic d'un groupe, il sera capable de prendre en charge le trafic minimal nécessaire pour la gestion des clés pour ce groupe.

GKMP fournit son propre contrôle d'accès, sur la base des certificats de permission signés à l'échelle du réseau. Cela dissémine partiellement la charge du contrôle d'accès et de la gestion des permissions. Une autorité à l'échelle du système doit allouer les certificats de permission, mais les décisions de contrôle d'accès au jour le jour sont de la responsabilité d'un GKMP.

2.3.5 Coûts de fonctionnement

Un site centralisé de distribution de clés contient, à un moment ou à un autre, les clés pour le réseau. C'est une cible précieuse des tentatives de compromission. Pour protéger ce site, des mécanismes de sécurité physiques et procéduraux sont employés (par exemple, des gardes, des barrières, des alarmes aux intrusions, double sauvegarde, pas de zone isolée). Ces mécanismes ne s'improvisent pas.

Permettre aux hôtes de créer et gérer leurs clés élimine le besoin d'un site centralisé de distribution de clés en ligne. L'approche du protocole restreint l'accès aux clés aux hôtes qui les utilisent (l'ensemble minimal). Comme les mécanismes de chiffrement auront déjà supporté les coûts de la sécurisation physique, il n'y aura pas d'autres coûts à ajouter au système du fait de la gestion de clés.

2.3.6 Ressources de communication

Comme un site centralisé est impliqué dans la création, la distribution, le changement des clés, et la fourniture du contrôle d'accès pour chaque groupe, il subit des accès fréquents. Les ressources de communication disponibles pour ce site deviennent souvent un goulet d'étranglement pour les groupes. Un gros tuyau est donc habituellement installé vers ce site.

Le protocole GKMP propose de déléguer la plus grande partie de la mission de création, distribution, changement de clés et de contrôle d'accès aux hôtes qui ont besoin des communications sécurisées. Il n'y a plus de tiers qui doive être consulté avant toute action de gestion de clé de groupe. Donc, les exigences de communications pour gérer les clés ont glissé jusqu'aux groupes eux-mêmes. Le besoin de communications à grande capacité particulières a donc été éliminé.

2.3.7 Fiabilité

Déléguer la responsabilité de la gestion des clés aux groupes élimine le site centralisé de gestion de clés comme point de défaillance central. Les groupes qui veulent utiliser la clé en sont responsables. Si le système de communications est défaillant pour la gestion des clés, il l'est aussi pour les communications.

Le protocole GKMP va tenter de déléguer autant de fonctions que possible au groupe. Il y aura des fonctions qui devront encore être effectuées en dehors du groupe (accorder des privilèges). Ces fonctions peuvent encore connaître des défaillances. GKMP va fonctionner sur le vieil ensemble de permissions. Ces fonctions n'ont pas besoin d'être en ligne. Elles sont effectuées indépendamment des actions de gestion de clé et ne sont pas cruciales pour le fonctionnement au jour le jour.

2.3.8 Sécurité

Les personnes sont l'élément qui fait courir le plus de risque à la sécurité. Un protocole réparti élimine de nombreuses personnes de la chaîne de distribution des clés. Cela limite "l'exposition" de la clé.

3. Généralités sur le protocole GKMP

3.1 Fonctions de soutien

Un protocole sûr de gestion de clés a besoin d'un certain nombre de fonctions de soutien, en particulier dans un environnement militaire. Les deux fonctions de soutien majeures sont la gestion de la sécurité et la gestion de groupe réseau. Dans le monde commercial, une compagnie pourra fournir ces fonctions de soutien.

La question pour la gestion de la sécurité est celle de la gestion des permissions ; dans un environnement militaire, la séparation des données se fait le long de lignes de classification classiques (c'est-à-dire, de TOP SECRET à NON CLASSÉ). Dans le monde commercial, ces niveaux sont confidentiel ou accès réservé.

La gestion de groupe réseau fournit une interface au système de communications et le contrôle des ressources du réseau. Certaines entités d'un système commercial ou militaire, l'hôte ou le centre des opérations du réseau, doivent fournir le protocole de gestion de clés avec une liste des membres du groupe. Aussi, si les ressources du réseau, bande passante et capacité de traitement, sont considérées comme rares, une structure de gestion doit faire leur répartition.

3.1.1 Gestion de la sécurité

La gestion de la sécurité est un rôle qui est tenu pour l'ensemble du réseau. Il implique des questions de gestion de permissions, d'initialisation de logiciels et de récupération de compromis à l'échelle du réseau. GKMP s'appuie sur la gestion de la sécurité pour son fonctionnement. Se référer à la figure 1 : Vue de la gestion de la sécurité.

GKMP doit supposer un traitement de confiance du logiciel du protocole avant et pendant l'installation. Si le GKMP doit utiliser le contrôle d'accès d'homologue à homologue, le système doit contrôler l'allocation des permissions. Ces permissions doivent être surveillées et mises à jour en tant que de besoin. Enfin, la surveillance de ces permissions doit inclure la maintenance d'une liste de révocation des certificats.

Démarrage sécurisé : on a besoin de contrôler le processus de chargement et d'initialisation du logiciel GKMP sur un hôte. Le protocole a besoin de clés, publiques et privées, pour fonctionner. Il doit aussi avoir des informations d'identité sur l'hôte au nom duquel il va agir.

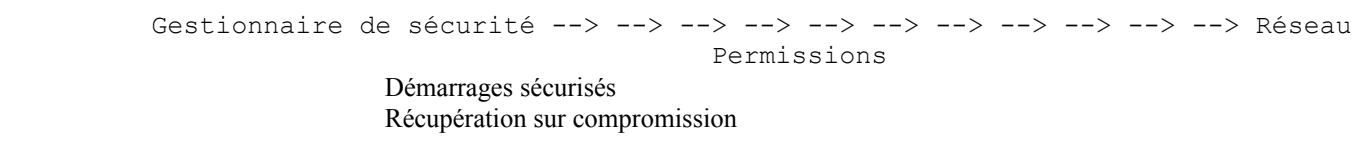

Figure 1 : Vue de la gestion de la sécurité

Il y a des problèmes de cycle de vie et de sécurité avec le logiciel pendant le transit, la mémorisation, la distribution, et l'installation. Une procédure de démarrage à usage unique doit vérifier l'identité de l'hôte. Des techniques physiques et de procédure d'identification vont vérifier l'identité de l'hôte (c'est-à-dire, la comptabilité du service de courrier des forces armées (ARFCS, *Armed Forces Courier Service*) ou une boîte aux lettres enregistrée). À la livraison des clés, le gestionnaire de la sécurité enregistre leur réception et assume la responsabilité de la clé.

Après l'installation appropriée du logiciel, une liasse papier vérifie le receveur. L'ordinateur va initialiser une association avec la fonction de gestion de la sécurité pour initialiser le logiciel du protocole (créer une paire unique de clés publique et privée pour le fonctionnement du réseau et recevoir les permissions réseau). Ce processus d'activation utilise les clés distribuées avec le logiciel (ce n'est valable que pour l'initialisation) pour sécuriser un échange avec le gestionnaire de la sécurité. L'hôte crée alors une paire unique de clés publique et privée et envoie la clé publique au gestionnaire de sécurité. Celui-ci crée un accréditif qui identifie de façon univoque l'hôte et ses permissions. Cet accréditif est signé par le gestionnaire de sécurité avec sa clé privée et peut être vérifié par tous les membres du réseau avec la clé publique.

Gestion des permissions : Chaque hôte sur le réseau reçoit un certificat de permissions, signé par le gestionnaire de sécurité, qui identifie de façon univoque cet hôte et les permissions d'accès qui lui sont allouées. Ces certificats de permission sont utilisés par les hôtes du réseau pour allouer des permissions aux autres hôtes.

Ce processus alloue les permissions aux équipements ou aux êtres humain conformément à leurs tâches. Ce processus implique des marges de sécurité et un jugement humain ; il sort donc du domaine d'application du protocole.

La fonction de gestion de la sécurité, en particulier dans les opérations militaires, serait chargée de la gestion des permissions et des classifications chez chaque hôte. Dans le monde du commerce, la gestion des permissions correspond aux projets ou aux tâches.

Gestion de la récupération des compromissions : Si un membre du groupe se trouve compromis, le protocole doit faciliter l'exclusion du membre compromis et revenir à un fonctionnement sûr. La fonction de gestion de la sécurité va fournir le contrôle de la récupération des compromissions.

Normalement, des techniques d'inspection physique ou de comptabilité trouvent les compromissions. Ces systèmes distincts font rapport des compromissions au système de gestion de clés. On doit supposer la perte de toutes les clés qui résident chez cet hôte. La fonction de gestion de la sécurité va annuler toutes les permissions allouées à cet hôte compromis. On crée une liste de tous les hôtes compromis connus et elle est distribuée à travers le réseau. Chaque hôte est alors chargé de revoir les propriétés de chaque association et de mettre en application le contrôle d'accès aux données.

3.1.2 Gestion du groupe

Le gestionnaire de groupe interagit avec les autres fonctions de gestion dans le réseau pour fournir à GKMP les listes de membres des groupes et les commandes pertinentes pour le groupe. GKMP ne traite strictement que de clés de chiffrement. Il s'appuie sur les services externes de communication et de gestion de réseau pour fournir les informations qui se rapportent au réseau. Principalement, il s'appuie sur le service de gestion de réseau pour lui fournir les adresses des membres du groupe (si le groupe est à l'initiative de l'envoyeur).

GKMP permet à une entité externe de déterminer le contrôleur d'un groupe. Le contrôleur du groupe devrait être capable de traiter les exigences supplémentaires de processus et de communication associées à ce rôle. Si ce n'est pas une fonction nécessaire dans une mise en œuvre, cette affectation des tâches de contrôleur peut être réglée à une valeur par défaut automatique. Cependant, même une entité de gestion externe par défaut détermine comment le rôle de contrôleur est alloué.

Le gestionnaire de groupe peut recevoir des rapports d'avancement de groupe du contrôleur de groupe. GKMP fournit un service au réseau. Il paraît sensé que quelqu'un dans le réseau soit intéressé par les progrès de ce service. GKMP peut fournir des rapports d'avancement. Il appartient à la gestion de réseau de déterminer la manière de faire ces rapports et leur destinataire. Se référer à la Figure 2 : interaction de gestionnaire de réseau.

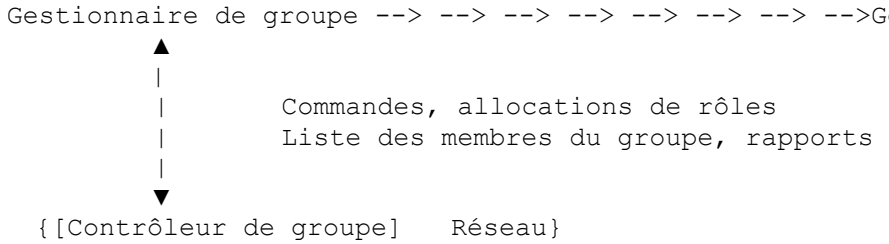

Figure 2 : Interaction de gestionnaire de réseau

Transposition de groupe à membre : Lorsque le GKMP est mis en œuvre dans le mode d'établissement de groupe initié par l'envoyeur, une liste des adresses des membres du groupe doit être fournie au titre de la commande d'établissement du groupe. GKMP va utiliser ces adresses pour contacter les membres du groupe et créer le groupe.

La création de groupes implique l'allocation d'une adresse de groupe, la mise à jour des bases de données de routeur, et la distribution de cette adresse de groupe aux membres du groupe. C'est une fonction classique de gestion de réseau. Le contrôleur de groupe GKMP sera un autre receveur de ces informations.

Allocation des rôles du protocole : Le protocole de gestion de groupe assigne des rôles aux membres d'un groupe particulier. Ces rôles sont binaires. Soit on a le contrôle sur le groupe, soit on est un membre d'un groupe. Une entité externe va allouer l'identité du contrôleur du groupe et du receveur du groupe. C'est un aspect souhaitable parce que certains ordinateurs sont plus capables que d'autres (c'est-à-dire, un site central, une grande quantité de puissance de calcul disponible pour le contrôle d'un groupe). On permet qu'une entité externe alloue ces rôles à des membres de groupe individuels, ceci est important dans les applications militaires du fait que dans une application commerciale, l'autorité allocataire et le contrôleur de groupe peuvent très bien être le même.

Rapports sur l'avancement des clés de groupe : Le protocole de gestion des clés de groupe doit être capable de faire rapport à quelqu'un. Si on crée un groupe, on devrait en faire rapport au demandeur du groupe. À l'inverse, si on n'est pas capable de créer un groupe, on devrait en faire rapport, en particulier parce que l'échec de création d'un groupe est à première vue tout au moins, très corrélé avec l'échec des communications sous-jacentes. Le protocole de gestion des clés de groupe n'a pas de capacité à réparer les communications sous-jacentes de sorte que la fonction de gestion de la communication doit traiter ces échecs.

```
Réseau = {[(Contrôleur du groupe 1) membres du groupe 1],
          [(Contrôleur du groupe 2) membres du groupe 2],
          [(Contrôleur du groupe 3) membres du groupe 3], }
```

Figure 3 : Gestion de groupe répartie

3.2 Rôles d'un protocole

La création et la distribution de clés de groupe exige l'assignation de rôles. Ces rôles identifient quelles fonctions effectuent les hôtes individuels dans le protocole. Les deux rôles principaux sont ceux de contrôleur et de receveur. Le contrôleur initie la création de la clé, forme les messages de distribution de la clé, et collecte les accusés de réception des clés de la part des receveurs. Les receveurs attendent un message de distribution, déchiffrent, valident, et accusent réception de la nouvelle clé.

Un des concepts essentiels de GKMP est la délégation du contrôle du groupe. Comme chaque hôte du réseau a la capacité d'agir comme contrôleur de groupe, les exigences de traitement et de communication du contrôle des groupes dans le réseau peuvent être réparties équitablement dans tout le réseau. Cela évite un point d'échec unique potentiel, l'encombrement des communications, et la surcharge des processeurs. Se reporter à la figure 3 : Gestion de groupe répartie.

3.2.1 Contrôleur d'un groupe

Le contrôleur de groupe est le membre du groupe qui a l'autorité pour effectuer les actions critiques du protocole (c'est-à-dire, créer les clés, distribuer les clés, créer les messages de changement de clés de groupe, et faire rapport sur les progrès de ces actions). Tous les membres du groupe ont la capacité d'être un contrôleur de groupe et pourraient assumer cette tâche si elle leur est allouée.

Le contrôleur de groupe aide à la constitution du groupe cryptographique et au maintien de la synchronisation des clés. Un groupe doit fonctionner sur les mêmes clés de chiffrement symétriques. Si une partie du groupe perd ou change sa clé de façon inappropriée, il ne sera plus capable d'envoyer ou recevoir des données à un autre hôte qui fonctionne sur la clé correcte. Donc, il est important que ces opérations de création ou de changement de clés soient sans ambiguïté et contrôlées (c'est-à-dire, il ne serait pas approprié que plusieurs hôtes essayent de changer simultanément les clés d'un réseau).

3.2.2 Receveur d'un groupe

Dit simplement, un receveur de groupe est tout membre de groupe qui n'agit pas comme le contrôleur. Les receveurs d'un groupe vont assister le contrôleur pour la création de clés, valider l'autorisation du contrôleur d'effectuer des actions, accepter la clé envoyée par le contrôleur, demander la clé au contrôleur, entretenir les listes de CRL locales, effectuer les vérification d'homologue des actions de gestion de clés, et gérer la clé locale.

3.3 Scénarios

3.3.1 Établissement d'un groupe

Le protocole pour établir un groupe d'hôtes qui partagent une clé de chiffrement doit créer une clé de grande qualité, vérifier que tous les receveurs prévus ont la permission de se joindre au groupe, distribuer la clé à tous les membres qualifiés, et faire rapport des progrès. Ce processus comporte deux phases : la création d'une clé, et la distribution de la clé. Voir la figure 4 : Établissement de groupe.

Le processus d'établissement du groupe est traité de la manière suivante. D'abord, une commande "créer le groupe" est produite auprès du commandant de groupe. Le contrôleur du groupe valide la commande pour s'assurer qu'elle vient d'un commandant autorisé et que le groupe est dans la gamme des permissions du commandant. Ensuite, le contrôleur crée une clé. Puis cette clé est passée aux membres du groupe, et enfin ils passent au processus de vérification d'homologue à homologue.

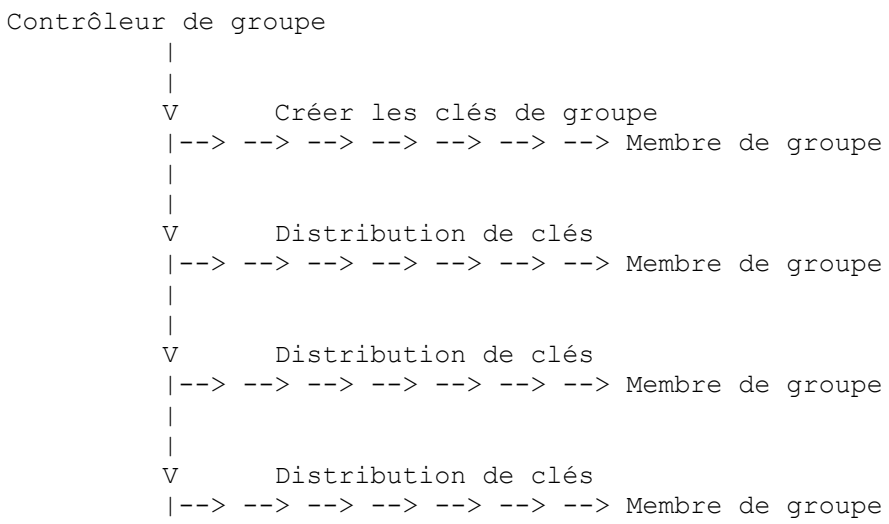

Figure 4 : Établissement de groupe

Valider la commande :
La commande Création de groupe est signée par le commandant de groupe (ce peut être dans le même appareil). Cette signature devrait être de nature asymétrique. La clé publique pour valider cette commande peut être envoyée avec la commande elle-même, si la clé publique est liée à l'identité du commandant.

Le contrôleur de groupe reçoit la commande. Il vérifie la signature, s'assurant par là que le message a été envoyé par la source alléguée et que le message n'a pas été modifié dans le transit.

Création de clés de groupe :
Le contrôleur initie la création de deux clés à utiliser dans le groupe. La création d'une clé de chiffrement exige que la clé soit suffisamment aléatoire. Les générateurs d'aléa, capables de créer des clés cryptographiques de grande qualité, tendent à être fondés sur des matériels spécialisés et ne seront vraisemblablement pas praticables pour ce protocole. Il y a plusieurs protocoles de création de clé établis qui sont fondés sur un logiciel (par exemple, Diffie-Hellman, FireFly, RSA). Tous ces algorithmes fondés sur un logiciel impliquent la coopération de deux hôtes pour créer une clé cryptographique. Ces algorithmes logiciels sont plus appropriés pour le présent protocole.

Aussi importante, dans la création de ces clés, est la vérification de l'autorisation du partenaire de la création de la clé. L'autorisation de posséder les clés inclut des permissions qui sont égales ou supérieures à celle du trafic du groupe et à la vérification d'identité.

Distribution des clés de groupe :
Le contrôleur distribue les clés de groupe aux membres du réseau. Le contrôleur doit vérifier l'identité et les permissions de chaque membre avant la distribution de la clé.

De la même façon, le membre du réseau doit vérifier l'identité du contrôleur, l'autorisation d'effectuer cette action, et les permissions.

La clé qui est distribuée est au même niveau que les données qu'elle va chiffrer. Donc, on doit chiffrer la clé durant sa

distribution. S'il n'existe pas de clé convenable entre le contrôleur et le membre, une nouvelle clé doit être créée. Cette nouvelle clé est créée de façon coopérative entre le contrôleur et le membre du réseau d'une façon similaire à celle des clés du réseau.

Le contrôleur crée un message à chiffrer sous la clé détenue par le contrôleur et le membre du réseau. Ce message comportera les informations de gestion des clés et les clés.

3.3.2 Changement de clés de groupe

Une clé de chiffrement a une durée de vie limitée. De nouvelles clés doivent remplacer les "vieilles" clés avant la fin de leur vie cryptographique. Ce processus est le changement de clés *(rekey)*.

Figure 5 : Changement de clés de groupe

Le changement de clés présente l'avantage d'utiliser une association cryptographique existante pour distribuer les clés. Il n'y a donc aucune exigence de vérification de l'identité et de l'autorisation pour les autres membres. Identité et autorisation sont supposées.

Un changement de clés de groupe comporte deux étapes. D'abord, le contrôleur de groupe crée de nouvelles clés de groupe. Ensuite, ces "nouvelles" clés sont envoyées aux membres du groupe dans un message en diffusion groupée. Voir la figure 5 : Changement de clés de groupe.
Création de clés de groupe :
Le contrôleur du changement de clés va créer les nouvelles clés exactement de la même manière que celle utilisée durant l'établissement du groupe.

Distribution des clés de groupe :
GKMP crée un message à l'adresse du groupe. Ce message utilise une des clés distribuées durant l'établissement du groupe pour chiffrer les nouvelles clés. Il contient aussi un jeton d'autorisation qui identifie le contrôleur comme l'agent du changement de clés et des nouvelles données de gestion. Tous les membres du groupe qui utilisent un protocole de diffusion groupée (s'il en existe un) acceptent ce message.

Le message qui change les clés du groupe chiffre les nouvelles clés avec la KEK existante. Comme tous les membres du groupe possèdent la KEK, le groupe entier peut déchiffrer ce message.

Le jeton qui autorise le contrôleur du groupe à effectuer ce changement de clés est aussi inclus. Ce jeton est signé de façon asymétrique par le commandant du groupe. Il identifie de façon univoque l'autorité du contrôleur du groupe pour changer les clés de ce groupe. Il identifie aussi pour le groupe le niveau de trafic et l'intervalle de changement de clés.

3.3.3 Suppression

Il peut être souhaitable d'être capable de supprimer des membres du groupe pour des raisons administratives ou de sécurité. La suppression administrative est la suppression d'un membre de confiance du groupe. Il est possible de confirmer la suppression de membres de confiance du groupe. La suppression qui relève de la sécurité est la suppression d'un membre qui n'est plus de confiance. On suppose que le membre va ignorer toutes les commandes de suppression.

Suppression administrative
La suppression administrative retire les clés du groupe aux membres de confiance du groupe. Cette suppression consiste en deux messages dont le premier envoie au groupe une commande chiffrée avec la TEK du groupe. La commande dit en substance : accusez réception puis supprimez les clés du groupe. Cette commande est signée du contrôleur du groupe pour empêcher les suppressions non autorisées.

Le message d'accusé de réception est aussi chiffré avec la TEK du groupe et il est envoyé pour accuser réception de la commande. On pourrait accuser réception de la réalisation de la commande si le réseau voulait accepter la charge de la création d'une paire de clés entre les membres existants du groupe et le contrôleur du groupe.

Récupération sur compromission
La récupération sur compromission est la suppression de membres du groupe qui ne sont plus de confiance. Cela implique en fait la création d'un groupe entièrement nouveau, sans les membres qui ne sont plus de confiance. Une fois que le nouveau groupe est créé, les opérations du réseau peuvent être basculées sur le nouveau groupe, refusant effectivement l'accès aux données du membre qui n'est plus de confiance.

Il y a toujours un compromis entre la sécurité et la poursuite des opérations du réseau lorsque un membre se trouve être compromis. La première position de la sécurité est que si un membre est compromis, le groupe doit être détruit et un nouveau groupe sûr doit ensuite être créé. Cependant, des soucis de fonctionnement peuvent parfois contrebalancer les questions de sécurité. La position du point de vue opérationnel est que le groupe va continuer de fonctionner avec le membre compromis et va glisser sur un nouveau groupe sûr lorsque il deviendra disponible.

GKMP ne rend obligatoire aucune des deux positions. Cependant, la vitesse et la souplesse de GKMP permet qu'un nouveau groupe sûr soit créé rapidement, réduisant par là les dommages potentiels causés par un membre compromis.

Une fois qu'un membre se trouve compromis, son certificat de membre est ajouté à une liste de révocation de certificats (CRL, *Certificate Revocation List*). La CRL est un ensemble de données signé de façon asymétrique par un gestionnaire de la sécurité. La liste est constituée par les identifiants des ressources compromises, une version de la CRL, et peut-être un identifiant du gestionnaire de sécurité. La CRL est consultée chaque fois qu'une nouvelle clé est négociée. Si un des créateurs de la clé est sur la CRL, la clé est détruite et l'interaction se termine.

L'idée derrière une CRL est que chaque hôte va garder des enregistrements de toutes les associations ouvertes et des ressources compromises. L'hôte va alors s'assurer qu'il n'a pas et ne va pas créer une association de sécurité ouverte avec quiconque est sur la CRL. Le concept de CRL devient plus compliqué dans le cas des groupes. Cela parce qu'il n'est pas nécessaire que chaque membre du groupe sache qui sont les autres membres du groupe. Donc, un membre d'un groupe n'a pas les informations suffisantes pour identifier les associations compromises avec le groupe. GKMP propose que les contrôleurs de groupe soient chargés de revoir la CRL et de prendre les mesures appropriées si un membre d'un groupe devait être compromis.

Une autre question qui se pose avec les CRL est la vitesse à laquelle elles peuvent être distribuée dans un réseau. Chaque fois qu'une clé est créée, les hôtes qui coopèrent échangent le numéro de version de leur CRL en cours. Si les versions ne correspondent pas, la version la plus récente est passée à l'hôte qui a la vieille version. Donc, les CRL se propagent lorsque des clés sont créées. Si cela est peu fréquent et si il y a un seul point d'insertion de CTL, la liste peut prendre plusieurs jours pour couvrir tout le réseau. GKMP permet une distribution plus rapide de la CRL.

GKMP délègue le contrôle des groupes à des contrôleurs de groupe spécifiques (un sous ensemble du réseau). Ces contrôleurs sont responsable du maintien de la sécurité du groupe. Si une distribution plus rapide de la CRL est désirée, le générateur de la CRL (la fonction de gestion de la sécurité) peut diffuser la CRL à ces contrôleurs. Les contrôleurs sont les points de l'activité de gestion des clés et sont les points de montage logiques des CRL.

4. Problèmes

Quels sont les problèmes non résolus de ce protocole ?

4.1 Contrôle d'accès

Une question intéressante d'un protocole de clés de groupe est celle du contrôle d'accès. Cela parce que on s'éloigne de la présence de personnes dans le circuit ou d'une autorité centrale pour vérifier les propriétés du groupe.

Le protocole de groupe doit se réguler lui-même. Il doit s'assurer que chaque membre d'un groupe satisfait à la politique classique de contrôle d'accès militaire (c'est-à-dire que le niveau de classification d'un membre du groupe doit être supérieur ou égal à la classification du groupe dans lequel il est).

L'allocation des permissions par une autorité supérieure est elle suffisante pour fournir le contrôle d'accès ? Ou un mécanisme plus discrétionnaire est-il nécessaire ?

4.2 MLS

GKMP doit être capable de fonctionner dans un environnement sûr à plusieurs niveaux. L'intégration d'un protocole de gestion de clés capable de créer des clés de plusieurs classifications différentes dans un système d'exploitation capable de

fonctionner avec plusieurs classifications n'est pas trivial.

On doit incorporer des normes d'étiquetage classifié. Les étiquettes de classification utilisées par le protocole de gestion de clés devraient coïncider avec les étiquettes utilisées par le système d'exploitation MLS. Ces questions d'interopérabilité doivent être examinées.

4.3 Conditions d'erreur

Un protocole de groupe est plus complexe qu'un protocole de paire de clés car il y a plus de conditions d'erreur possibles. Dans un protocole de paire de clés, on a deux parties ; elles doivent communiquer entre elles. Il est relativement simple de définir et tenir compte de toutes les conditions d'erreur potentielles.

Une hypothèse de tout protocole de groupe est que l'Internet sous-jacent est, dans une certaine mesure, toujours cassé. Le concepteur du protocole doit supposer que les messages seront retardés ou détruits dans le transit, les membre ne vont pas tous recevoir tous les messages en diffusion groupée, et l'accusé de réception des actions peut n'être pas livré. Cette hypothèse est importante si un protocole utilise des fonctions de diffusion groupée pour accélérer les actions.

Le protocole doit fournir des mécanismes de récupération pour permettre aux membres du groupe de récupérer de la perte de messages. Il doit récupérer d'une façon transparente pour l'hôte et le réseau de communications sous-jacent.

Par exemple, il y a la question de savoir si on peut ou non créer un accusé de réception de couche application des actions de diffusion groupée. La question est en rapport avec la bande passante nécessaire pour les accusés de réception. Il peut être moins douloureux pour les systèmes de communications sous-jacents que chaque membre identifie les erreurs potentielles et les corrige directement. La tâche de traitement des conditions d'erreur dans un protocole de gestion de clés est doublement difficile parce que de nombreuses conditions d'erreur peuvent être induites (invoquées par un tiers qui essaye de casser la sécurité de ce système) pour récupérer les clés qui sont en transit ou de bloquer la dissémination d'une clé, attaquant par là le mécanisme.

4.4 Commercial ou militaire

La gestion de clés commerciale et militaire diffère par de nombreux aspects. Les protocoles de gestion de clés commerciaux tendent à mettre l'accent sur l'interopérabilité, la liberté d'action, et la performance. Les systèmes militaires tendent à privilégier la sécurité et le contrôle du fonctionnement.

Il y aura une différence dans les algorithmes de chiffrement. Le protocole militaire va certainement utiliser un chiffrement de niveau élevé à cause de la protection d'informations classifiées. Le système commercial va probablement utiliser des algorithmes et des techniques certifiées pour des systèmes de communication non classifiés. La principale différence est dans la longueur et le type des algorithmes.

Un protocole militaire va exiger plus de gestion et de structure qu'un protocole commercial. Le militaire a toujours adopté une structure hiérarchique de communications et le système commercial, en particulier si on regarde l'Internet, fonctionne principalement dans un style anarchiste.

4.4.1 Type d'algorithme

Une autre différence entre gestion de clé militaire et commerciale est le type des algorithmes de chiffrement. Le monde commercial utilise des algorithmes de chiffrement comme DES et à l'avenir Skipjack. Les militaires utilisent d'autres algorithmes de chiffrement qui diffèrent par la longueur des clés et ont plus de restrictions. Un exemple en serait l'identification de ACCORDION comme algorithme de chiffrement de clé militaire, comme celui utilisé dans le programme EKMS de la NSA.

Toute expérience avec un protocole de gestion de clés de groupe doit prendre en considération les différences entre les algorithmes militaires et commerciaux. Les algorithmes commerciaux tendent à être plus rapides à mettre en œuvre, à aller plus vite, à consommer moins de temps de traitement, et à permettre un fonctionnement non classifié. Cependant, on doit veiller à ne pas peindre un tableau irréaliste des performances des protocoles fondés sur ces algorithmes commerciaux. Un algorithme militaire tend à être plus difficile à mettre en œuvre, lent de fonctionnement, à exiger plus de bande passante, un certain nombre de caractéristiques déplaisantes du point de vue commercial, mais cela permet un plus haut degré de sécurité cryptographique. Une façon de traiter de la disparité entre les algorithmes est d'utiliser les algorithmes de chiffrement commerciaux et de donner aux champs la taille utilisée par les algorithmes cryptographiques comparables du Ministère de la Défense pour insérer les délais pour simuler les temps de traitement des algorithmes du DOD.

4.4.2 Philosophie de la gestion

La gestion pour un réseau militaire est beaucoup plus structurée que pour un réseau commercial. Un réseau militaire va restreindre la création des groupes réseau, les changements de clés de ces groupes, et l'accès aux données contenues dans ces groupes. À l'opposé, le monde commercial va permettre à tout membre du réseau de créer un groupe et permettre à tout autre membre du réseau de se joindre à ce groupe.

Le protocole de gestion de clés de groupe doit permettre ces deux architectures, c'est-à-dire, une qui permet une hiérarchie très structurée de contrôle des commandes et une autre qui laisse libre la création de groupes.

4.5 Fonctionnement à l'initiative du receveur

Comment cela fonctionne réellement, quels sont les compromis sur les performances ? des expérimentations sont nécessaires.
Qui est le pilote du groupe ?
Comment choisit-on un nouveau pilote ?
Peut-on avoir plusieurs pilotes ?
Le contrôle d'accès fondé sur des règles permettra t-il une discrimination assez fine de l'accès ?

Les méthodes de dissémination de GKP/GRP réparties doivent être examinées. Cela inclut :
- o de résoudre les questions d'identification de groupe, telles que comment notifier aux membres potentiels les exigences pour l'adhésion sans compromettre des informations de sécurité pertinentes sur le groupe ;
- o les approches pour l'identification rapide des sources GKP/GRP doivent être développées, telle qu'un "ARP de clé" par lequel un nouveau membre diffuse dans le groupe une demande de service de clés et les membres existants résolvent qui fournit le service ;
- o les effets pour la sécurité de la distribution des décisions de contrôle d'accès doivent aussi être revus.

5. Considérations pour la sécurité

Le présent document, est entièrement consacré aux problèmes de sécurité.

6. Adresse des auteurs

Hugh Harney
SPARTA, Inc.
Secure Systems Engineering Division
9861 Broken Land Parkway, Suite 300
Columbia, MD 21046-1170
USA
téléphone : +1 410 381 9400 (ext. 203)
mél : hh@columbia.sparta.com

Carl Muckenhirn
SPARTA, Inc.
Secure Systems Engineering Division
9861 Broken Land Parkway, Suite 300
Columbia, MD 21046-1170
USA
téléphone : +1 410 381 9400 (ext. 208)
mél : cfm@columbia.sparta.com