Infrastructure sécurisée de routage multipoint: le point de vue de l'opérateur réseau

Zainab Khallouf[aß], Vincent Roca[ß], Renaud Moignard[a], Sébastien Loye[a]

[a]*France Télécom R&D, DAC/CPN, 2, avenue Pierre-Marzin-22307 Lannion cedex.*
E-Mail: prénom.nom@rd.francetelecom.com
[ß]*INRIA Rhône Alpes (projet Planète), 655 avenue de l'Europe; Montbonnot; 38334 St Ismier Cedex.*
E-Mail : prénom.nom@inria.fr

Les fondements du multicast IP sont définis depuis plusieurs années et pourtant à ce jour très peu de déploiements à grande échelle ont eu lieu dans les réseaux opérationnels. L'une des raisons essentielles au non déploiement du multicast chez les opérateurs réseaux est la problématique de la sécurité. Or, lorsqu'on l'on parle de sécurité appliquée au domaine du multicast, deux niveaux complémentaires doivent être considérés: d'une part la sécurité applicative, qui vise à assurer la protection et la confidentialité des flux échangés au sein d'un groupe, et qui intéresse essentiellement les fournisseurs de contenu et les clients finaux; d'autre part la sécurité de l'infrastructure de routage multicast qui est du ressort de l'opérateur réseau. Cet article se focalise sur ce deuxième point et définit le point de vue de l'opérateur, propose une taxonomie des attaques auxquelles il s'expose, et discute les grandes classes de solutions envisageables.

Mots clés: Communications de Groupe, Multicast IP, Sécurité, Attaques sur l'infrastructure, Déni de Service

1. Introduction

Le multicast IP est un modèle de diffusion efficace des données permettant à une source d'émettre une seule copie de trafic à destination de plusieurs récepteurs dispersés sur l'Internet. Le modèle de service initial, tel qu'il a été introduit par Deering [1], est le modèle ASM (Any-Source Multicast). Ce modèle permet à n'importe quel terminal de s'abonner à un groupe, d'envoyer et de recevoir des flux multicast. Récemment, un modèle simplifié a été proposé au sein de l'IETF (Internet Engineering Task Force), le modèle SSM (Source Specific Multicast) spécialement conçu pour supporter la diffusion de type <1 vers n>. Ce modèle introduit la notion de canal qui est l'association d'une adresse de groupe G et de l'adresse S de la source du trafic multicast.

Pour que le modèle de diffusion fonctionne, deux composants ont été définis. Tout d'abord, à l'accès du réseau, un protocole de souscription / résiliation à des groupes permet à un terminal de spécifier le trafic qu'il désire recevoir. Il s'agit du protocole IGMP (Internet Group Management Protocol) [1] en IPv4 et MLD (Multicast Listener Discovery) [2] en IPv6. Ensuite, des protocoles de routage multicast dans le cœur de réseau permettent de construire les arbres de distribution le long desquels est acheminé le trafic des sources vers les membres du groupe. Ces protocoles de routage multicast peuvent être classés en deux catégories, selon qu'ils sont propres à un "domaine multicast" (c'est le cas de MOSPF, CBT, PIM-SM [3] et PIM-DM) ou qu'ils sont inter-domaines (comme MBGP/PIM-SM/MSDP [4] et BGMP [5]).

Bien que le modèle de diffusion multicast ait été défini depuis plusieurs années et les implantations de la famille de protocole multicast soient disponibles dans presque tous les équipements réseau, à ce jour cette technologie n'est pourtant pas mise en œuvre et déployée à grande échelle dans les réseaux des opérateurs. Plusieurs raisons permettent d'expliquer cet état de fait, tels

que le problème de l'allocation dynamique des adresses multicast, la fiabilité de transmission ou la sécurité. Cet article n'abord que la problématique de sécurité.

En pratique, lorsque l'on parle de la sécurité appliquée au domaine du multicast, deux niveaux complémentaires doivent être considérés: la sécurité applicative d'une part, qui vise à la protection des données, et la sécurité de l'infrastructure de routage IP multicast de l'opérateur d'autre part.

La première problématique a été largement étudiée [6] [7] [8] et plusieurs travaux ont été réalisés au sein du groupe de travail MSEC [9] à l'IETF pour garantir une sécurité des données multicast transportées. Malgré l'efficacité de ces travaux, il est important de souligner que ces flux sécurisés sont transportés par l'infrastructure réseau multicast, qui elle n'est pas sécurisée et donc vulnérable aux attaques, en particulier aux attaques par déni de service (ou DoS). Le principe de ces attaques est de submerger le réseau de trafic pollueur ou de requêtes, afin de saturer la bande passante des liens ou les capacités de traitement des équipements (routeurs, serveurs), et rendre le réseau indisponible. Tous les services, y compris les services "non multicast", sont alors impactés.

Les attaques DoS sont nombreuses et variées, certaines exploitent la vulnérabilité du protocole IGMP de souscription à un groupe de diffusion, d'autres ciblent les protocoles de routage multicast intra-domaine comme PIM-SM ou inter-domaine tels MSDP et BGMP. Enfin, d'autres types d'attaques, délibérées ou non, peuvent provenir d'un comportement non conforme du contrôle de congestion de l'application.

On voit que le niveau de sécurité exigé de la part de l'opérateur de réseau, qui gère et exploite l'infrastructure de routage multicast, diffère largement de la sécurité de bout en bout de niveau application. C'est l'objet de ce papier que de se focalise sur la sécurité de l'infrastructure réseau et la problématique de l'opérateur réseau.

Cet article est organisé comme suit : la section 2 identifie et analyse les différents acteurs impliqués dans un service de diffusion multicast d'un contenu. Cette analyse est illustrée par deux études de cas complémentaires: un service de diffusion vidéo sur ADSL, et un service de diffusion libre. À la lumière de cette discussion, la section 3 analyse les spécificités et exigences de sécurité de l'opérateur réseau. La section 4 classifie les attaques possibles sur l'infrastructure, tandis que la section 5 présente les grandes familles de solutions possibles pour sécuriser cette infrastructure. La section 6 offre une discussion critique des problèmes et des solutions proposées, qui reposent souvent sur des hypothèses peu réalistes dans notre contexte. Finalement nous concluons.

2. Les différents acteurs dans le cadre d'un service de diffusion multicast

2.1. Vue générale

Comprendre la problématique de sécurité de l'infrastructure réseau nécessite de comprendre la façon dont l'architecture de service elle-même est organisée, d'identifier les différents acteurs qui collaborent à la fourniture du service de diffusion multicast, et de comprendre leurs relations, contractuelles ou non. Dans cet article nous distinguons (Figure 1) :

- L'Opérateur Réseau

  C'est celui qui possède, déploie et gère l'infrastructure physique (c'est à dire les routeurs multicast, les NAS/BAS (Network Access Server/Broadband Access Server), les DSLAMs (Digital Subscriber Line Multiplexer), etc.). L'opérateur met en œuvre le routage multicast et met en oeuvre des relations de peering avec les autres opérateurs (pour échanger les paires de source/groupe avec MSDP). L'opérateur fournit physiquement l'accès multicast IP à l'utilisateur final mais il est important de souligner qu'il n'a pas de relations commerciales avec celui-ci.
- Le Fournisseur d'Accès Internet (ou ISP) et le Fournisseur de Service

  L'ISP a la charge des relations commerciales, relativs à l'accès réseau, avec l'utilisateur final. Il fournit l'accès, la connectivité Internet et les services associés (courrier, portail web, messagerie instantanée).

Le fournisseur de service quant à lui est chargé de la définition et de la commercialisation de l'offre de service (diffusion de TV numérique, ou VoD) à l'utilisateur final, et possède aussi à ce titre une relation avec l'utilisateur final.

Ces deux rôles peuvent être joués par un seul et même acteur. Dans ce papier nous utiliserons le terme *générique* de "Fournisseur de Service" pour désigner l'un ou l'autre de ces fournisseurs.

- Le fournisseur de contenu

  Cette entité fournit les informations et le contenu qui composent le service proposé aux utilisateurs finaux par le fournisseur de service. Ce contenu peut être du texte, des images, de la vidéo (TV ou VoD numérique), ou de l'audio (radio, musique).
- L'agrégateur de contenu

  Cette entité construit les bouquets de chaînes à partir du contenu fourni par un ou plusieurs fournisseurs de contenu. Il collecte le contenu, applique le codage approprié sur ce contenu et le diffuse à partir de son réseau. L'agrégateur de contenu a des relations de peering et des contrats avec un ou plusieurs opérateurs de réseau afin d'atteindre les utilisateurs finaux.
- L'utilisateur final

  L'utilisateur possède un terminal multimédia qui peut être un PC ou un ensemble TV/ Set Top Box. En premier lieu, l'utilisateur obtient un accès Internet de la part de son ISP, ensuite il peut utiliser le service de diffusion multicast proposé par l'opérateur réseau afin de s'abonner aux chaînes/groupes qu'il désire, et ainsi recevoir le contenu associé.

Notons, qu'un même acteur peut très bien jouer le rôle de plusieurs entités.

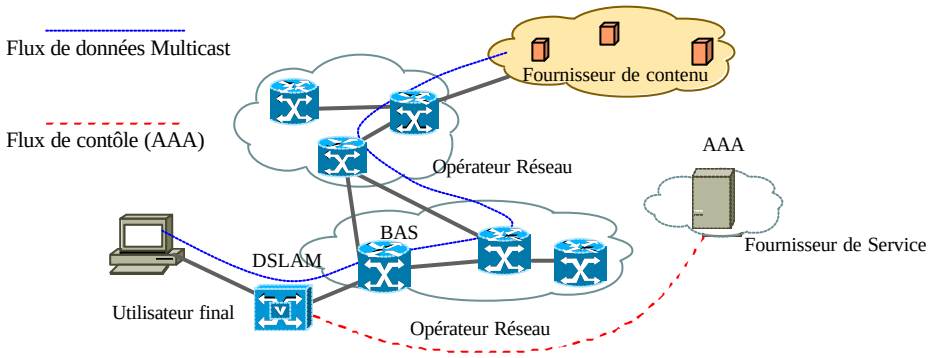

Figure 1 : les différents acteurs dans la chaîne fournisseur de contenu ➔ utilisateurs finaux

2.2. Premier exemple : service commercial de TV sur ADSL

Cette section décrit un service commercial de multicast de TV sur ADSL (Asymmetric Digital Subscriber Line). En pratique, dans ce type de service le Fournisseur de Service offre l'accès Internet haut débit au client et gère les aspects d'identification, authentification, autorisation, allocation d'adresse IP et facturation. Ce premier niveau d'authentification/autorisation permet au client d'obtenir un accès Internet à haut débit.

Il est probable que l'accès à certains contenus (telles les chaînes TV hertziennes) restera gratuit avec l'ADSL. En revanche l'accès à des chaînes à péage ou à des services comme la vidéo à la demande (VoD) sont des services payants soumis à un contrôle d'accès auprès d'un serveur d'authentification comme le serveur RADIUS (Remote Access Dial In User Service).

Afin de recevoir les flux vidéo, le client utilise IGMP (avec IPv4) ou MLD (avec IPv6). Les messages "IGMP reports" sont traités par les équipements multicast du réseau de l'opérateur réseau, à savoir le DSLAM ou le BAS (en fonction de la maturité des fonctions multicast de ces équipements ou des choix d'ingénierie opérationnelle). Les flux multicast sont donc transmis à partir du réseau de l'agrégateur de contenu, puis transitent sur le réseau de l'opérateur réseau avant d'atteindre le client final. Les flux de gestion, tels que les flux AAA (Authorization/ Authentication/ Accounting) qui

permettent d'authentifier et de facturer l'utilisateur, sont échangés et relayés entre l'opérateur de réseau et le fournisseur de service. Ce sont les seuls flux qui existent entre le client et le fournisseur de service.

2.3. Deuxième exemple: diffusion libre d'un contenu gratuit

Dans le cas de la diffusion libre d'un contenu (logiciels gratuits, vidéo clips, visio-conférence entre amis, etc.), la chaîne de bout en bout (Fournisseur de contenu ➔ utilisateurs finaux) est toujours valide. En revanche le client n'a pas à s'authentifier pour recevoir le contenu. Dans ce schéma de service, il n'y a qu'un seul niveau d'authentification, lors de l'obtention de la connectivité Internet.

3. Sécurité de l'infrastructure du point de vue de l'opérateur réseau

L'opérateur réseau a un point de vue très spécifique sur la sécurité de son réseau :

Le service de communication de groupe fourni à ses clients (utilisateurs finaux, opérateurs réseaux avec lesquels il a des relations de peering, agrégateur de contenu) doit être opérationnel en permanence, en dépit des anomalies pouvant survenir, que celles-ci soient intentionnelles (attaques) ou non (dysfonctionnement d'un composant quelconque, chez l'utilisateur ou l'opérateur). La sécurité n'est pas un but en soi, mais un moyen d'atteindre l'objectif de « continuation de service envers et contre tout ». D'autre part, les mesures de sécurité mises en œuvre ne doivent pas influencer négativement les performances des services unicast et multicast fournis par l'opérateur.

L'opérateur réseau peut avoir des exigences supplémentaires en matière de sécurité. Il peut vouloir garantir que le trafic échangé ne soit pas modifié lorsqu'il transite sur son propre réseau. Il peut aussi vouloir garantir un certain niveau de confidentialité au trafic, au cas où un attaquant puisse écouter le trafic à partir d'un lien ou d'un routeur corrompu. Ces considérations de sécurité supplémentaires ne sont cependant pas l'objectif premier de l'opérateur réseau, et sont mieux adressées par la sécurité de bout en bout. Par conséquent nous ne les considérons pas dans cet article.

De même, les pannes physiques affectant des liens, des équipements, routeurs ou serveurs, ne sont pas considérées dans cet article, bien qu'elles aient un impact fort par rapport à l'objectif de « continuité de service » de l'opérateur. Notons que notre définition partage quelques similitudes avec celle de « survivabilité du réseau » [10], même si cette dernière est un peu plus large puisqu'elle inclut les pannes matérielles.

4. Taxonomie des attaques intéressant l'opérateur réseau

Le modèle de diffusion multicast IP est par définition un modèle ouvert, où n'existe aucun mécanisme de contrôle à l'accès du réseau. Or, plusieurs attaques récentes, tel le ver Ramen [11], ont clairement montré la vulnérabilité de l'infrastructure multicast aux attaques, en particulier les attaques DoS. Dans cette section nous présentons une taxonomie des attaques dirigées contre l'infrastructure de l'opérateur :

- ***Selon leur origine:*** ces attaques peuvent provenir soit du cœur de réseau soit de l'accès. Le réseau de cœur contient l'ensemble des routeurs multicast qui exécutent les protocoles de routage multicast. En revanche, le réseau d'accès est schématiquement constitué des équipements de concentration de trafic qui opèrent IGMP/MLD, et des utilisateurs finaux.
- ***Selon leur type:*** on peut distinguer les attaques dirigées dans le plan de transfert (échange de données) des attaques dirigées dans le plan de contrôle (visant les protocoles).

A chaque fois le terme "attaque" est à prendre au sens large et dénote soit une agression intentionnelle, soit non intentionnelle.

4.1. Attaques internes

Une attaque interne provient d'un élément de l'arbre de distribution multicast de l'opérateur réseau : routeur corrompu ou lien réseau piraté. Ces attaques exploitent les vulnérabilités des

équipements physiques au sein du réseau, comme les routeurs et les serveurs. En prenant le contrôle d'un équipement du réseau, un intrus peut alors déclencher une variété d'attaques.

4.1.1 Attaques internes dirigées dans le plan de transfert

Les attaques dans le plan de transfert sont nombreuses : un intrus peut modifier le contenu des paquets, ou submerger le réseau par du trafic parasite qui va être reçu par tous les récepteurs ; il peut aussi copier le contenu d'un groupe, interpréter les informations et les rejouer plus tard. Ces attaques, qui pénalisent essentiellement les clients et fournisseurs de contenu, ont aussi des conséquences directes pour l'opérateur puisqu'elles génèrent des flux parasites qui gaspillent de la bande passante et rendent le réseau lent ou indisponible.

Des attaques passives, où l'attaquant profite de son contrôle sur un routeur corrompu pour espionner le trafic, ne mettent pas en péril le fonctionnement du réseau de l'opérateur mais affectent la crédibilité de l'opérateur auprès de ses clients fournisseurs de service.

4.1.2 Attaques internes dans le plan de contrôle

Les protocoles de routage en général, et ceux de routage multicast en particulier, sont très vulnérables aux attaques face à un intrus stratégiquement placé, car en pratique les messages de contrôle ne sont pas authentifiés dans les réseaux opérationnels. Cet intrus peut alors créer, rejouer, espionner, ou supprimer des messages de routage, ce qui entraîne rapidement des dénis de service pour les utilisateurs finaux.

Le protocole PIM-SM [3] par exemple, est vulnérable aux attaques basées sur des messages de contrôle falsifiés [3] [12]. Ainsi un faux message (Join/Prune) peut diriger les flux multicast vers des récepteurs illégitimes. Un intrus ayant pris le contrôle d'un routeur peut, en injectant de faux paquets de contrôle, modifier les tables de routage multicast afin de submerger de trafic un routeur particulier. L'attaque est d'autant plus grave que le routeur victime est stratégique (ce peut être le RP).

4.2 Attaques venant de la périphérie

Aucun mécanisme de contrôle d'accès n'étant assuré par le modèle traditionnel ASM (et guère plus avec le modèle SSM), un intrus peut facilement exploiter cette faiblesse pour déclencher des attaques très graves pour le réseau de l'opérateur. C'est ce que nous abordons dans cette section.

4.2.1 Attaques périphériques dans le plan de transfert

On doit distinguer les attaques venant des sources de celles venant des récepteurs.

- *Attaques issues des sources*

Le modèle ASM est très vulnérable aux attaques DoS (et DDoS). Avec ce modèle ouvert, un intrus peut inonder le réseau de l'opérateur par des flux multicast. Ces attaques qui pénalisent essentiellement les clients finaux et fournisseurs de contenu ont aussi des conséquences directes pour l'opérateur réseau puisqu'elles génèrent des flux parasites qui gaspillent de la bande passante et rendent le réseau lent ou indisponible.

Et une attaque de ce type, qui commence dans le plan de transfert, peut facilement affecter le plan de contrôle. Ainsi générer du trafic destiné à un grand nombre de groupes distincts, existants ou non, peut épuiser les ressources du RP, et si le routage inter-domaines est actif, l'infrastructure est alors submergée de messages MSDP de type « Source Active ». C'est ce qui s'est passé avec le vers "Ramen" [11].

Le modèle SSM est plus robuste face à ces attaques. Pourtant il reste vulnérable face un intrus qui se fait passer pour une source légitime en lui piratant son adresse IP. Comme le routage multicast basé sur l'algorithme RPF (Reverse Path Forwarding) offre une certaine protection contre des sources qui modifient leur adresse IP source (les paquets arrivant sur une interface différente de celle qui serait utilisée pour atteindre la source sont rejetés), pour réussir son attaque l'intrus doit être sur le plus court chemin vers la source authentique. Cela rend l'attaque plus compliquée à conduire mais ne l'empêche pas totalement.

- *Attaques issues des récepteurs*

Les modèles ASM et SSM n'ont aucun mécanisme de contrôle d'accès coté récepteurs. Un intrus peut facilement utiliser IGMP/MLD pour joindre un grand nombre de flux multicast existant, ce qui consomme de la bande passante de réseau de l'opérateur .

Une autre possibilité vient des protocoles de contrôle de congestion des applications multicast Actuellement plusieurs protocoles sont en cours de standardisation à l'IETF: WEBRC [13] pour les protocoles de multicast fiable multi-débit (tel ALC), PGMCC [14] et TFMCC pour les protocoles de multicast fiables du type PGM ou NORM. En cas de défaillance (volontaire ou non), un récepteur peut demander plus de trafic que raisonnable, en évitant de réagir aux indications de congestion, perturbant ainsi les flux réactifs tels TCP. Ceci est d'autant plus inquiétant qu'un récepteur est incité à se conduire ainsi puisque c'est une façon d'obtenir plus que sa part équitable de la bande passante.

4.2.2 Attaques périphériques dans le plan de contrôle

Ces attaques exploitent les vulnérabilités des protocoles IGMP et MLD. Elle peuvent consister à générer un grand nombre de messages IGMP de type REPORT; ou bien générer des messages IGMPv1 (ancienne version) et ainsi forcer les routeurs à basculer dans le mode de compatibilité, bien moins efficace ; ou encore générer une succession de messages REPORT suivis de messages LEAVE, ce qui a pour effet de forcer les équipements à passer par une nouvelle phase de scrutation afin de déterminer s'il reste ou non des récepteurs pour ce groupe (forcer le basculement en mode IGMPv1 amplifie encore cette attaque). Bien entendu ces attaques peuvent se faire de façon distribuée, et l'adresse source de ces messages sera bien souvent usurpée.

5. Taxonomie des mécanismes de protection de l'infrastructure de l'opérateur réseau

Nous nous intéressons maintenant aux techniques de défense. Nous pouvons distinguer deux catégories : les solutions préventives qui visent à renforcer la sécurité en amont, et les solutions réactives qui prennent des mesures correctives afin d'assurer une continuité de service.

5.1 Mécanismes de défense préventifs

Les mécanismes de défense préventifs visent à ne permettre qu'aux seules entités autorisées de construire les branches des arbres de diffusion multicast et ainsi de participer à la diffusion.

- *Protection de l'arbre de diffusion multicast*

Protéger l'arbre de diffusion multicast consiste à protéger les messages de contrôle échangés entre routeurs multicast afin d'assurer que les branches des arbres ne lient strictement que les entités (routeurs et récepteurs) autorisées [15]. Dans ce contexte, plusieurs protocoles cryptographiques ont été proposés pour réaliser l'authentification, l'intégrité, la non répudiation et la confidentialité des messages de contrôle [16]. La majorité de ces protocoles utilisent la cryptographie asymétrique (type "signature numérique") pour authentifier les paquets de contrôle. Ces protocoles ont l'inconvénient d'entrainer des traitements supplémentaires importants qui dégradent les performances et peuvent également introduire d'autres types d'attaques DoS, telle que l'inondation par des faux messages (qui devront être vérifiés de toute façon).

Protéger l'arbre de diffusion nécessite également de contrôler les utilisateurs en introduisant des mécanismes d'authentification à IGMP ou MLD [17] [18] [19]. Les mêmes remarques quant à la charge CPU nécessaire au traitement de ces informations d'authentification peuvent être faites ici.

- *Prévention des attaques DoS*

Mettre en place des mesures afin d'empêcher ou limiter les effets des attaques DoS est une mission cruciale pour l'opérateur réseau. Ceci est généralement fait en appliquant des politiques pour gérer la consommation de ressources dans le réseau, afin de garantir que les clients légitimes qui respectent les termes de leur contrat ne soient pas affectés par les attaques [20] [21]. Ces mécanismes peuvent être couplés avec des mécanismes de contrôle d'accès. Les techniques de prévoyance telles que le marquage de paquets [22], le filtrage en entrée/sortie des files d'attente des routeurs et le filtrage en

fonction de la route sont des mécanismes importants afin de se défendre contre les attaques DoS. En général ces travaux ont été faits pour les communications point à point, et à notre connaissance aucune étude sur l'efficacité de ces mécanismes dans une infrastructure multicast n'a été réalisée.

5.2 Mécanismes réactifs

Concevoir et réaliser un système résistant à toute attaque est mission impossible, puisque les attaques évoluent, sont de plus en plus innovantes et leur dangerosité ne fait qu'augmenter. Le réseau de l'opérateur doit donc être en mesure de tolérer les attaques qui n'auront pu être parées par les mécanismes préventifs, et assurer ainsi une continuité de service. Ces mécanismes réactifs sont en fait une combinaison de techniques de reconnaissance et détection de trafic malicieux (IDS) et de techniques de protection/restauration qui permettent au réseau de « survivre » à l'attaque.

- *Systèmes de détection d'intrusion (IDS)*

La détection d'intrusion a pour objectif de détecter toute violation de la politique de sécurité d'un système informatique. Elle permet ainsi de détecter les attaques (en temps réel ou en différé) portant atteinte à la sécurité de ce système. Plusieurs solutions ont été proposées afin de sécuriser l'infrastructure de routage unicast [23]. Mais aucune d'elle n'a été faite dans le contexte du multicast qui soulève beaucoup de défis, en particulier pour collecter de façon automatisée les données représentant l'activité des systèmes de routage [24].

- *Mécanismes de continuité de service*

Plusieurs techniques permettent d'assurer la continuité de service et préserver le réseau dans le cas où l'intrus réussit à violer toutes les mesures précédentes :

- *Limitation de débit :* le principe consiste à limiter le débit des flux considérés suspects par les mécanismes IDS. Bien que largement utilisée, cette solution a des limites. Ainsi elle permet des attaques distribuées, même si chacun des flux "malicieux" est individuellement limité en débit. De plus le paramétrage de la limitation en débit n'est pas chose aisée et nécessite de définir des seuils appropriés, statiques ou dynamiques.
- *Filtrage :* on se sert de la politique de sécurité définie par l'administrateur réseau, ou des signaux reçus de la part d'un système IDS, pour bloquer les flux considérés non conformes. Ces mécanismes sont largement utilisés, mais ont à leur tour des limitations puisque d'une part il y a un risque de filtrer des flux légitimes, et d'autre part un attaquant peut utiliser ces mécanismes de filtrage comme un outil pour déclencher une attaque DoS [21].
- *Mécanismes d'isolement des attaques :* Ces techniques réagissent aux attaques en modifiant la topologie réseau, soit en ajoutant des ressources supplémentaires, soit en isolant les parties du réseau victimes de l'attaque et en basculant le service vers les parties « saines ». Dans [10] l'auteur propose une architecture pour tolérer les attaques au sein de communications de groupe et formalise le problème comme un problème d'optimisation multidimensionnel. Ces techniques peuvent généralement être implantées efficacement en utilisant un réseau MPLS (Multiprotocol Label Switching).

6. Discussion sur les attaques et les techniques de défense

Nous avons jusqu'ici identifié les attaques possibles et les divers mécanismes de sécurité. Cette section apporte une discussion critique complémentaire, tout d'abord en classant les attaques selon leur dangerosité et probabilité, ensuite en soulignant les limites de certaines approches de sécurité qui reposent sur des hypothèses qui s'appliquent difficilement au contexte de l'opérateur réseau.

6.1 Classification des attaques selon leur dangerosité relative

Les attaques discutées en section 4 peuvent être classées en fonction de leur dangerosité relative pour le réseau de l'opérateur (ordre décroissant) :

- *Attaques venant de la périphérie : (*en excluant les attaques de type contrôle de congestion)

Ces attaques, qu'elles visent le plan de contrôle ou de transfert, sont faciles à lancer mais très difficiles à éviter (ainsi générer un grand nombre des requêtes IGMP peut créer une attaque DoS même si IGMP est sécurisé). Les attaques survenues sur MSDP ont également montré la fragilité de l'infrastructure multicast vis-à-vis des attaques DoS venues de la périphérie.

- *Attaques sur le protocole de contrôle de congestion :*
  Mettre en œuvre des mécanismes de contrôle de congestion est indispensable, mais ces mécanismes, implantés dans les applications, sont également facilement modifiables. De plus des utilisateurs seront incités à rendre leur flux non (ou moins) réactifs aux indications de congestion puisqu'ils bénéficieront d'un meilleur service au détriment des autres flux type TCP. Ceci a un impact direct sur le réseau de l'opérateur.
- *Attaques internes :*
  Lancer ces attaques nécessite en général de disposer d'un emplacement stratégique au sein du réseau de l'opérateur, ce qui est peu probable.

En pratique, un opérateur réseau doit se focaliser essentiellement sur les attaques périphériques, très faciles à lancer et qui peuvent avoir des conséquences sérieuses sur son réseau. Se prémunir contre les attaques sur les routeurs internes et l'infrastructure physique n'est pas une priorité et ne devrait être entrepris que dans une deuxième étape.

6.2 Authentification et autorisation des participants à une session multicast

Nous examinons maintenant d'un œil critique certaines des hypothèses faites par ceux qui proposent des mécanismes de sécurité.

De nombreux travaux liés à la sécurité de l'infrastructure multicast partent du principe que les participants à une session multicast sont authentifiés et autorisés [27]. En fait, ces hypothèses sont rarement valides ou effectives :

- L'authentification/autorisation suppose que le client soit enregistré dans un serveur d'authentification (par exemple de type RADIUS). C'est vrai dans le cadre d'une offre de service commerciale (TV sur ADSL), mais cette hypothèse est irréaliste si l'on veut permettre des services de diffusion libres (ainsi organiser une visio-conférence entre amis, section 2.3) où aucune inscription préliminaire n'est nécessaire.
- L'authentification/autorisation est seulement possible si une coopération opérateur/fournisseur de service existe puisque l'opérateur de réseau doit interroger ou accéder à la base de données « client » du fournisseur de service. Ceci sera impossible dans certaines situations (ainsi si l'opérateur joue seulement un rôle de transit).
- Rien ne garantit qu'un client authentifié/autorisé se comportera correctement. Un client peut exploiter les vulnérabilités de certaines applications de façon à lancer des attaques sur le protocole de contrôle de congestion, ou bien simplement être victime d'un virus (un cheval de Troie, ou un root-kit installé sur le PC du client) qui lui-même profitera de l'authentification/autorisation du client pour lancer une attaque DoS.
- En présence de mécanismes de translation d'adresses NAT/PAT (Network Address Translation, Port Address Translation), l'authentification/autorisation du client sur la base de l'adresse IP est inefficace car l'adresse IP de la machine terminale est masquée au réseau de l'opérateur. Prenons le cas d'un utilisateur qui se connecte via sa passerelle domestique faisant du NAT et qui a construit un réseau local sans fil. Dès que cet utilisateur a rejoint le service de communication de groupe, tous les flux issus de sa passerelle sont considérés légitimes. Cependant un utilisateur dans le voisinage peut joindre ce réseau sans fil (les réseaux 802.11b sont connus pour avoir des failles de sécurité) et en profiter pour lancer une attaque DoS.

6.3 Modification des protocoles existants

Certaines propositions de sécurisation modifient les protocoles multicast existants [18], en ajoutant par exemple des mécanismes dauthentification à IGMPv3, ou définissent même de nouveaux protocoles de routage sécurisés, comme KHIP [27] qui s'appuie sur une variante du protocole CBT

[26] (protocole qui n'a pourtant jamais été ni implanté ni déployé dans les réseaux opérationnels). Même si ces nouveaux protocoles sont extrêmement robustes à certains types d'attaques, ces solutions ne sont pas réalistes et n'ont pratiquement aucune chance d'être un jour déployées par un opérateur de réseau, très attentif à modifier le moins possible son infrastructure et ses protocoles réseau existants. En outre, même si une proposition est standardisée à l'IETF, il lui reste un long chemin à parcourir avant d'être déployée largement dans les réseaux opérationnels, et se posera alors le problème de l'interopérabilité avec des réseaux tiers qui n'ont pas migré vers la version sécurisée du protocole en question.

6.4 Confiance/dépendance entre domaines multicast

Un opérateur de réseau est responsable du niveau et de la qualité de service offert à ses clients. Aussi, des solutions de sécurité nécessitant la collaboration de plusieurs opérateurs réseau pour la création d'arbres multicast inter-domaines sont difficiles à mettre en place et à déployer. Par conséquent, les exigences de sécurité d'un opérateur réseau, telles que définies dans la section 3, doivent être essentiellement égocentriques et ne pas être dépendantes d'autres opérateurs réseau.

7. Conclusions

Ce travail cible la sécurité de l'infrastructure multicast du point de vue de l'opérateur réseau. Ses exigences de sécurité sont largement différentes de celles des utilisateurs finaux ou des fournisseurs de service. Ainsi est-il essentiellement préoccupé par une exigence de « continuité de service », notamment lorsque son réseau est victime d'une attaque. L'opérateur est en fait tout particulièrement attentif aux points suivants:

- prévenir (ou diminuer les risques) d'attaques qui menacent son infrastructure réseau,
- se défendre contre les éventuelles attaques,
- construire une infrastructure qui soit robuste aux attaques.

L'infrastructure de l'opérateur est particulièrement vulnérable aux attaques DoS qui consomment des ressources de bande passante et compromettent les capacités de traitement des routeurs. Ces attaques DoS, intentionnelles ou non, sont faciles à lancer par des utilisateurs localisés à la périphérie du réseau de l'opérateur. L'opérateur doit donc porter tous ses efforts afin de se prémunir de ces attaques.

En revanche, vouloir sécuriser les protocoles de routage multicast dans le réseau coeur de l'opérateur afin d'éviter qu'un routeur corrompu n'altère les arbres de distribution multicast a une importance très secondaire puisque cette attaque est hautement improbable.

Plusieurs hypothèses couramment faites doivent aussi être évitées. En premier lieu, sécuriser IGMP par une authentification/autorisation systématique du client n'est ni toujours possible, ni efficace (un utilisateur légitime et authentifié peut conduire des attaques s'il est par exemple infecté par un virus). En second lieu, proposer des modifications à des protocoles existants largement déployés n'est pas efficace car les opérateurs, très conservateurs, recherchent avant tout des solutions pratiques et réalistes plutôt que des solutions intellectuellement idéales.

8. Références

1. Steve Deering. *"Host Extensions for IP Multicasting"*. Request for Comment (RFC) 1112, August 1989.
2. Steve Deering, Bill Fenner, and Brian Haberman. *"Multicast listener discovery (MLD) for IPv6"*. Request for Comments (RFC): 2710, October 1999.
3. Deborah Estrin, Dino Farinacci, Ahmed Helmy, David Thaler, Steven Deering, Mark Handley, Van Jacobson, Ching-gung Liu, Puneet Sharma, Liming Wei, *"Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification"*. Request for Comment 117, June 1997.
4. Bill Fenner, Dave Thaler. *"The multicast source discovery protocol (MSDP)"*. Request for Comment (RFC) 3618, October 2003.
5. Dave Thaler. *"Border gateway multicast protocol (BGMP): Protocol specification"*. IETF INTERNET-DRAFT draft-ietf-bgmp-spec-06.txt, 19 January 2004.

6. Suvo Mittra. *"Iolus: A framework for scalable secure multicasting"*. Proceedings of the ACM SIGCOMM '97 conference on Applications, technologies, architectures, and protocols for computer communication, Cannes, France, Pages: 277 – 288, Year of Publication: 1997, ISSN: 0146-4833.
7. Chung Kei Wong, Mohamed Gouda, and Simon S.Lam. *"Secure group communications using key graphs"*. ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication, Vancouver, British Columbia, Canada, Pages: 68 – 79, Year of Publication: 1998, ISSN: 0146-4833.
8. Ran Canetti, Juan A. Garay, Gene Itkis, Daniele Micciancio, Moni Naor, Benny Pinkas. *"Multicast Security: A Taxonomy and Some Efficient Constructions"*. INFOCOM 1999: New York, NY, USA - Volume 2, Pages: 708-716.
9. Multicast security (MSEC) working group.http://www.ietf.org/html.charters/mseccharter.html.
10. William Yurcik, David Tipper. *"A survivability framework for connection-oriented group communications"*. IEEE Pacific Rim International Symposium on Dependable Computing 2000 (PRDC 2000), University of California at Los Angeles (UCLA) USA, Dec. 2000.
11. Prashant Rajvaidya, Krishna Ramachandran, and Kevin C. Almeroth, *"Detection and deflection of dos attacks against the multicast source discovery protocol"*. Technical report, Department of Computer Science, University of California, Santa Barbara, July 2002. http://www.caida.org/tools/measurement/Mantra/mantra-publications/mantra-publications.html
12. Thomas Hardjono, Brad Cain. *"PIM-SM security: Interdomain issues and solutions"*. In Communications and Multimedia Security CMS, Leuven, BELGIUM, September 1999.
13. Michael Luby, Vivek Goyal. *"Wave and equation based rate control building block"*, IETF INTERNET-DRAFT Reliable Multicast Transport (RMT) draft-ietf-rmt-bb-webrc-04.txt, December 2002. Work in progress. Expire June 2003.
14. L. Rizzo, G. Iannaccone, L. Vicisano, and M. Handley. *"Pgmcc single rate multicast congestion control: Protocol Specification"*. IETF INTERNET-DRAFT draft-ietf-rmt-bb-pgmcc-01.txt, 27 June 2002. Work in progress. Expires: December 2002.
15. Robert K. Wysocki, Thomas Hardjono, Lakshminath R. Dondeti. *"Multicast and Group Security"*. Artech House, Incorporated, ISBN 1-58053-342-6, 2003, 334 pp.
16. David B. Johnson, Yih-Chun Hu, Adrian Perrig. *"Efficient security mechanisms for routing protocols"*. In The 10th Annual Network and Distributed System Security Symposium, San Diego, California, February 2003.
17. Tony Ballardie and Jon Crowcroft. *"Multicast-specific security threats and counter-measures"*. In Symposium on Network and Distributed System Security (SNDSS'95), San Diego, February1995.
18. Paul Judge, Mostafa Ammar. *"Security issues and solutions in multicast content distribution: A survey"*, IEEE Network magazine special issue on Multicasting, page 30, January/February 2003.
19. A. Van Moffaert and O. Paridaens. *"Security issues in Protocol Independent Multicast - Sparse Mode (PIM-SM)"*, IETF INTERNET-DRAFT draft-irtf-gsec-pim-sm-security-issues-00.txt, December, 2001. Work in progress. Expires June, 2002.
20. Jelena Mirkovic, Janice Martin, and Peter Rei-her, *"A taxonomy of ddos attacks and ddos defense mechanisms"*. Technical Report CSD-TR-0200180, University of California, Los Angeles, 2002.
21. Aman Garg, A. L Narasimha Reddy. *"Mitigating denial of service attacks using QoS regulation"*. In Tenth International Workshop on Quality of Service (IWQoS 2002), Miami Beach, USA, May 2002.
22. Kihong Park and Heejo Lee. *"On the effective-ness of probabilistic packet marking forIP traceback under denial of service attack"*. In INFOCOM 2001, Alaska, USA, April 2001.
23. Feiyi Wang. *"Vulnerability Analysis, Intrusion Prevention and Detection for Link State Routing Protocols"*, PhD thesis, Carolina State University, Dec.2000.
24. Adams, T. Bu, R. Caceres, N. Duffield, T. Friedman, J.Horowitz, F. Lo Presti, S. Moon, V. Paxson, and D. Towsley. *"The use of end-to-end multicast measurements for characterizing internal network behavior"*, IEEE Communications Magazine, May 2000.
25. Antonio Gomez-Skarmeta and Angel L. Mateo and Pedro M. Ruiz, *"IGMPv3-based method for avoiding DoS attacks in Multicast-Enabled Network"*, 25th Annual IEEE Conference on Local computer Networks (LCN'00), November 08 - 10, 2000, Tampa, Florida.
26. A. Ballardie. *"Core based trees (CBT) multicast routing architecture"*, Request for Comments (RFC) 2201, September 1997.
27. Clay Shields, J. J. Garcia-Luna-Aceves. *"Khip- a scalable protocol for secure multicast routing"*. In ACM SIGCOMM'99 Computer Communication Review, Cambridge, Massachusetts, United States, Pages: 53 – 64, 1999.