

Union internationale des télécommunications

**UIT-T**

SECTEUR DE LA NORMALISATION  
DES TÉLÉCOMMUNICATIONS  
DE L'UIT

**X.1244**

(09/2008)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION  
ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberspace – Lutte contre le pollupostage

---

**Aspects généraux de la lutte contre le spam  
dans les applications multimédias IP**

Recommandation UIT-T X.1244



RECOMMANDATIONS UIT-T DE LA SÉRIE X  
**RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ**

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
<b>Lutte contre le pollupostage</b>	<b>X.1230–X.1249</b>
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339

*Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.*

## **Recommandation UIT-T X.1244**

### **Aspects généraux de la lutte contre le spam dans les applications multimédias IP**

#### **Résumé**

La Recommandation UIT-T X.1244 spécifie les concepts de base, les caractéristiques et les aspects techniques liés à la lutte contre le spam dans les applications multimédias IP (téléphonie IP, messagerie instantanée, etc.). Les divers types de spam d'application multimédia IP sont classés par catégories et pour chaque catégorie, on décrit les caractéristiques. Cette Recommandation décrit diverses menaces de sécurité liées au spam d'application multimédia IP. Différentes techniques ont été mises au point pour venir à bout du spam de courrier électronique, qui est devenu un problème de société. Certaines de ces techniques peuvent être utilisées dans le cas du spam d'application multimédia IP. Cette Recommandation analyse les mécanismes classiques de lutte contre le spam et examine leur applicabilité dans le cas du spam d'application multimédia IP. Enfin, elle mentionne quelques éléments à prendre en considération pour la lutte contre le spam d'application multimédia IP.

#### **Source**

La Recommandation UIT-T X.1244 a été approuvée le 19 septembre 2008 par la Commission d'études 17 (2005-2008) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

#### **Mots clés**

Spam de messagerie instantanée, spam d'application multimédia IP, spam, spam de téléphonie IP

## AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

## NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

## DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2009

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

## TABLE DES MATIÈRES

	<b>Page</b>
1	Domaine d'application ..... 1
2	Références..... 1
3	Définitions ..... 1
3.1	Termes définis ailleurs ..... 1
3.2	Termes définis dans la présente Recommandation ..... 2
4	Abréviations et acronymes ..... 3
5	Conventions ..... 4
6	Concept et types courants de spam multimédia IP ..... 5
6.1	Spam de VoIP..... 5
6.2	Spam de messagerie multimédia IP..... 5
6.3	Spam de messagerie instantanée ..... 6
6.4	Spam de bavardage..... 6
6.5	Spam multimodal..... 6
6.6	Spam de service de partage de fichier de type P2P..... 7
6.7	Spam de site web ..... 7
7	Classification des spams multimédias IP..... 7
7.1	Spam vocal en temps réel ..... 8
7.2	Spam textuel en temps réel..... 9
7.3	Spam vidéo en temps réel..... 9
7.4	Spam vocal pas en temps réel..... 9
7.5	Spam textuel pas en temps réel ..... 10
7.6	Spam vidéo pas en temps réel ..... 10
8	Aspects techniques liés à la lutte contre le spam multimédia IP ..... 10
8.1	Création et transmission de spams ..... 11
8.2	Détection et filtrage des spams..... 12
8.3	Mesures à prendre concernant les spams reçus ..... 13
9	Menaces de sécurité liées au spam ..... 13
9.1	Menaces de sécurité liées au spam ..... 13
9.2	Classification des menaces de sécurité liées aux spams..... 15
9.3	Contremesures ..... 16
10	Applicabilité de mécanismes connus de lutte contre le spam au cas des applications multimédias IP..... 17
10.1	Filtrage par identification ..... 18
10.2	Masquage d'adresse ..... 20
10.3	Preuve interactive pour les personnes ..... 21
10.4	Filtrage du contenu ..... 21
10.5	Authentification par échange de clé ..... 22
10.6	Filtrage du spam dans le réseau..... 23

	<b>Page</b>
10.7	Timbre en ligne..... 24
10.8	Filtrage du spam basé sur une autorisation..... 24
10.9	Action en justice et réglementation ..... 25
11	Considérations relatives à la lutte contre le spam d'application multimédia IP ..... 26
11.1	Utilisateur de service (abonné à un service)..... 26
11.2	Fournisseur de service ..... 27
11.3	Opérateur de réseau ..... 28
11.4	Organisme public..... 28
11.5	Autres considérations ..... 29
	Bibliographie..... 30

## **Introduction**

Le spam de courrier électronique pose un problème de société. Diverses solutions ont été élaborées et mises en œuvre pour résoudre ce problème, mais aucune d'entre elles n'a réellement permis de l'éliminer. Les applications multimédias IP comportent plusieurs types de services, comme la téléphonie IP, la messagerie instantanée, etc. Ces services multimédias IP deviennent une nouvelle cible pour les spammeurs, car l'envoi de spams dans ces services est plus simple sur le plan technique et meilleur marché. Il faut étudier la question du spam d'application multimédia IP avant que celui-ci ne devienne un problème pour le grand public.

La présente Recommandation décrit le concept et les caractéristiques de divers types de spam que l'on peut rencontrer dans les applications multimédias IP. Elle examine certains aspects techniques et de sécurité liés à la lutte contre le spam d'application multimédia IP, puis mentionne quelques éléments que plusieurs membres participant à la fourniture de services multimédias IP (fournisseurs de service, utilisateurs de service, etc.) doivent prendre en considération pour lutter contre le spam d'application multimédia IP.



# Recommandation UIT-T X.1244

## Aspects généraux de la lutte contre le spam dans les applications multimédias IP

### 1 Domaine d'application

La présente Recommandation contient une présentation générale du spam multimédia IP et porte plus précisément sur les éléments suivants:

- concept et caractéristiques du spam multimédia IP;
- aspects techniques liés au spam multimédia IP;
- menaces de sécurité liées au spam;
- méthodes de lutte contre le spam et leur applicabilité dans le cas du spam multimédia IP;
- divers éléments à prendre en considération pour lutter contre le spam dans les applications multimédias IP.

NOTE – L'utilisation du terme "identité" dans la présente Recommandation ne lui confère pas une valeur absolue, et ne constitue pas en particulier une validation positive.

### 2 Références

Aucune.

### 3 Définitions

#### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

**3.1.1 liste de contrôle d'accès (ACL, *access control list*)** [b-UIT-T X.741]: cet attribut sert à contenir les identités d'initiateurs qui reçoivent soit une autorisation spécifique d'accès à des informations de gestion ou un refus spécifique d'accès à des informations de gestion.

**3.1.2 autorité de certification (CA, *certification authority*)** [b-UIT-T X.509]: autorité jouissant de la confiance d'un ou de plusieurs utilisateurs pour la création et l'attribution de certificats de clé publique. L'autorité de certification peut, de manière optionnelle, créer les clés des utilisateurs.

**3.1.3 conférence** [b-UIT-T T.124]: ensemble de nœuds qui sont liés et capables d'échanger des informations audiographiques et audiovisuelles à travers divers réseaux de communication.

**3.1.4 courrier identifié par clés de domaine (DKIM, *domain keys identified mail*)** [b-IETF RFC 4871]: mécanisme de signature cryptographique des messages de courrier électronique, permettant à un domaine signataire de revendiquer être responsable de l'introduction d'un message dans le flux de courriers. Les destinataires du message peuvent vérifier la signature en interrogeant directement le domaine du signataire pour extraire la clé publique appropriée, et confirmer ainsi que le message a été attesté par une entité possédant la clé privée du domaine signataire.

**3.1.5 messagerie instantanée (IM, *instant messaging*)** [b-IETF RFC 3428]: échange de contenus entre un ensemble de participants presque en temps réel. Les contenus sont généralement des messages de texte courts, mais ce n'est pas nécessairement le cas.

**3.1.6 relation entre deux entités homologues (P2P, *peer-to-peer*)** [b-UIT-T T.180]: dans une telle relation, les utilisateurs peuvent négocier les caractéristiques de leur interaction auxquelles ils devront ensuite se conformer pour communiquer, sachant que les deux utilisateurs (une entité et son homologue) ont potentiellement les mêmes droits. Le document [b-IETF RFC 4981] indique que les

réseaux P2P sont ceux qui présentent les trois caractéristiques suivantes: auto-organisation, communication symétrique et commande répartie.

**3.1.7 PGP (Pretty Good Privacy)** [b-IETF RFC 1991]: protocole utilisant clé publique et chiffrement classique pour assurer des services de sécurité pour les fichiers de données et les messages de courrier électronique. Ces services incluent la confidentialité et la signature numérique. Le protocole PGP a été créé par Philip Zimmermann et a été publié pour la première fois (version 1.0) en 1991. D'autres versions, par exemple PGP ouvert qui est décrit dans le document [b-IETF RFC 4880], ont ensuite été conçues et mises en œuvre dans le cadre d'une collaboration uniquement entre volontaires conformément aux indications données par Philip Zimmermann. *PGP et Pretty Good Privacy sont des marques déposées de Philip Zimmermann.*

**3.1.8 infrastructure de clé publique (PKI, public key infrastructure)** [b-UIT-T X.509]: infrastructure pouvant prendre en charge la gestion de clés publiques afin de fournir des services d'authentification, de chiffrement, d'intégrité et de non-répudiation.

**3.1.9 sécurité de la couche de transport (TLS, transport layer security)** [b-UIT-T Q.814]: le protocole TLS fournit en option la confidentialité des communications. Ce protocole permet aux applications client/serveur de communiquer de manière à empêcher toute écoute illégale, altération ou intrusion. Le protocole TLS permet également d'assurer une authentification forte entre homologues et l'intégrité des flux de données.

## **3.2 Termes définis dans la présente Recommandation**

La présente Recommandation définit les termes suivants:

**3.2.1 spam d'appât:** découlant de l'analogie avec la pêche (et l'hameçonnage (voir § 3.2.10)), un spam d'appât est un type de spam contenant un élément, par exemple un objet de courrier électronique ou un lien intégré, destiné à attirer les utilisateurs. L'utilisateur attiré est attaqué par le spam d'appât.

**3.2.2 blog:** contraction de "web log", un blog est une liste en ligne, éventuellement multimédia, d'intérêts personnels de son propriétaire qui est mise à la disposition du grand public pour visualisation et, parfois, pour amélioration.

**3.2.3 bot, robot:** programme qui fonctionne comme un agent pour un utilisateur ou un autre programme afin de simuler une activité humaine.

**3.2.4 empoisonnement de cache DNS:** technique qui consiste à faire croire à un serveur de noms de domaine (serveur DNS) que l'adresse DNS d'un serveur donné a changé alors qu'en réalité il n'en est rien. Une fois que le serveur DNS a été empoisonné, cette information est généralement mise en mémoire cache pendant un certain temps, de sorte que les utilisateurs du serveur subissent aussi les effets de l'attaque.

**3.2.5 message multimédia IP:** message de texte, vocal ou vidéo qui est transmis et stocké dans un terminal ou un serveur multimédia IP dans l'attente d'être consulté par son destinataire. Il est l'équivalent pour le service multimédia IP du message vocal pour le service téléphonique.

**3.2.6 spam multimédia IP:** messages ou appels non sollicités dans des applications multimédias IP. Pour le distinguer du spam classique de courrier électronique, le spam multimédia IP désigne le spam sur les nouvelles méthodes de télécommunication sur IP, telles que les services de messagerie instantanée (IM), de présence ou de téléphonie IP (VoIP).

**3.2.7 modalité:** ce terme est généralement employé pour désigner les formes, protocoles ou conditions applicables aux communications formelles. Dans le contexte de la présente Recommandation, il désigne le ou les codages des informations, dont certaines sont perceptibles par l'être humain. Comme exemples de modalité, citons les données textuelles, graphiques, audio, vidéo ou haptiques utilisées dans les interfaces homme-ordinateur. Les informations multimodales peuvent avoir pour origine ou pour destination des dispositifs multimodaux. Comme exemples

d'interfaces homme-ordinateur, citons les microphones pour la saisie de données vocales (sonores), les stylets pour la saisie de données haptiques, les claviers pour la saisie de données textuelles, les souris pour la saisie de données de mouvement, les haut-parleurs pour la restitution de signaux de synthèse vocale, les écrans pour l'affichage de données graphiques/textuelles, les vibreurs pour le retour haptique et les systèmes d'écriture braille pour malvoyants.

**3.2.8 message multimodal:** message multimédia contenant des informations codées différemment pour une interaction via plusieurs modalités. Par exemple, un message MMS (service de messagerie multimédia) peut acheminer des modalités textuelles, graphiques et audio. Une page web peut aussi avoir un contenu modal multimédia (par exemple texte et vidéo). De même, un courrier électronique peut contenir une pièce jointe graphique conjointement avec du texte. Ainsi, la multimodalité permet à l'utilisateur de choisir une modalité préférée en fonction de l'environnement, de la commodité ou du contenu.

**3.2.9 jeu en ligne:** jeu en temps réel auquel on joue sur les réseaux.

**3.2.10 hameçonnage, phishing:** tentative d'obtention illicite et frauduleuse d'informations sensibles (nom d'utilisateur, mot de passe, données de compte bancaire, etc.) en se faisant passer pour une entité digne de confiance dans une communication électronique.

**3.2.11 détournement de session:** mécanisme consistant à voler une session d'utilisateur valable pour accéder de façon non autorisée à des informations ou à des services.

**3.2.12 spam de messagerie instantanée (SPIM, *spam over instant messaging*):** spam visant des utilisateurs d'un service de messagerie instantanée.

**3.2.13 spam de téléphonie Internet (SPIT, *spam over Internet telephony*):** spam visant des utilisateurs d'un service de téléphonie Internet.

**3.2.14 spammeur:** expéditeur de spams.

**3.2.15 envoi de spams, spamming:** chaîne d'activités réalisées par des spammeurs pour envoyer des spams (établissement de listes de cibles, création de spams, distribution de spams, etc.).

**3.2.16 spimmeur:** expéditeur de SPIM.

**3.2.17 spitteur:** expéditeur de SPIT.

**3.2.18 contenu créé par l'utilisateur (UCC, *user created content*):** toute forme de contenu (vidéo, blog, images, audio, etc.) créé par des utilisateurs finaux (personnes lambda) pour être mis à la disposition du grand public.

**3.2.19 contenu généré par l'utilisateur (UGC, *user generated content*):** équivalent à UCC.

**3.2.20 hameçonnage vocal, vishing:** accès illégal à des informations personnelles et financières privées par le biais du service de téléphonie IP (VoIP). Le terme "vishing" est une contraction de "voice phishing".

## 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ACL	liste de contrôle d'accès ( <i>access control list</i> )
APEC	Organisation de coopération économique Asie-Pacifique ( <i>Asia-Pacific Economic Cooperation</i> )
ARP	protocole de résolution d'adresse ( <i>address resolution protocol</i> )
ASCII	code normalisé américain pour l'échange d'informations ( <i>american standard code for information interchange</i> )
CA	autorité de certification ( <i>certificate authority</i> )

DB	base de données ( <i>database</i> )
DKIM	courrier identifié par clés de domaine ( <i>domain keys identified mail</i> )
HTTP	protocole de transfert hypertexte ( <i>hypertext transfer protocol</i> )
IM	messagerie instantanée ( <i>instant messaging</i> )
IP	protocole Internet ( <i>Internet protocol</i> )
TVIP	télévision IP
IPv4	version 4 du protocole Internet ( <i>Internet protocol version 4</i> )
IPv6	version 6 du protocole Internet ( <i>Internet protocol version 6</i> )
IRC	service de bavardage Internet ( <i>Internet relay chat</i> )
ISP	fournisseur de service Internet ( <i>Internet service provider</i> )
ITSP	fournisseur de service de téléphonie Internet ( <i>Internet telephony service provider</i> )
IVR	réponse vocale interactive ( <i>interactive voice response</i> )
MAC	commande d'accès au support ( <i>media access control</i> )
MIPv4	IPv4 mobile ( <i>mobile IPv4</i> )
MIPv6	IPv6 mobile ( <i>mobile IPv6</i> )
NDP	protocole de découverte de voisin ( <i>neighbor discovery protocol</i> )
OS	système d'exploitation ( <i>operating system</i> )
P2P	relation d'homologue à homologue ( <i>peer-to-peer</i> )
PGP	Pretty Good Privacy
PKI	infrastructure de clé publique ( <i>public key infrastructure</i> )
RTPC	réseau téléphonique public commuté
RTP	protocole de transport en temps réel ( <i>real-time transport protocol</i> )
SMS	service de messages courts ( <i>short message service</i> )
SMTP	protocole simple de transfert de courrier ( <i>simple mail transfer protocol</i> )
SQL	langage de requête structuré ( <i>structured query language</i> )
TCP	protocole de commande de transmission ( <i>transmission control protocol</i> )
TLS	sécurité de la couche de transport ( <i>transport layer security</i> )
URI	identificateur uniforme de ressource ( <i>uniform resource identifier</i> )
URL	localisateur uniforme de ressource ( <i>uniform resource locator</i> )
VoD	vidéo à la demande ( <i>video on demand</i> )
VoIP	téléphonie IP ( <i>voice over IP</i> )

## 5 Conventions

Aucune.

## **6 Concept et types courants de spam multimédia IP**

Il n'existe aucune définition du spam convenue à l'échelle mondiale, mais ce terme est habituellement utilisé pour désigner des télécommunications électroniques de masse non sollicitées par courrier électronique ou par messagerie mobile pour promouvoir des produits ou des services commerciaux. Actuellement, le spam n'est pas limité au courrier électronique ou à la messagerie mobile. Il gagne les applications multimédias IP comme la VoIP et la messagerie instantanée. Le spam multimédia IP peut être défini comme des télécommunications électroniques de masse non sollicitées dans des applications multimédias IP pour promouvoir des produits ou des services commerciaux. Des spams d'application multimédia IP peuvent être rencontrés sur divers types d'applications multimédias IP comme la VoIP et la messagerie instantanée.

Le présent paragraphe contient une liste des types courants de spam multimédia IP que l'on peut rencontrer dans les applications multimédias IP et décrit les caractéristiques de chacun de ces types de spam.

### **6.1 Spam de VoIP**

Les spams de VoIP, transmis par les services de VoIP, sont des spams vocaux en temps réel, par exemple des appels de télémarketing, qui reposent sur des communications avec un télévendeur et sur une interaction avec des systèmes IVR (réponse vocale interactive). Comme les services de télémarketing utilisant des services de VoIP se généralisent rapidement du fait du déploiement rapide des services de VoIP dans le monde entier, les spams de VoIP constituent une menace de plus en plus importante. En effet, il n'est pas difficile de lancer des appels en masse. Il est possible de recruter des télévendeurs dans des pays où la main-d'œuvre est meilleur marché que dans le pays cible, étant donné que le coût des appels internationaux a considérablement baissé avec l'utilisation des services de VoIP. Il est très facile pour les spammeurs de collecter des informations sur les utilisateurs d'application multimédia IP cibles. Tous ces facteurs font que le spam de VoIP peut poser un problème aux fournisseurs et aux utilisateurs de services de VoIP.

### **6.2 Spam de messagerie multimédia IP**

Un message multimédia IP est un message de texte, vocal ou vidéo qui est transmis et stocké dans un terminal ou un serveur multimédia IP dans l'attente d'être consulté par son destinataire. Il est l'équivalent pour le service multimédia IP du message vocal pour le service de téléphonie. Un spam de messagerie multimédia IP est un spam qui utilise le service de messagerie multimédia IP. Son destinataire le vérifie et le supprime, de la même manière qu'un spam de courrier électronique ou de messagerie mobile. Un grand nombre de terminaux prenant en charge des applications multimédias IP, tels que les téléphones VoIP, assurent des fonctions de messagerie multimédia, ce qui en fait des applications cibles pour les expéditeurs de spams de messagerie multimédia IP.

Les spams de messagerie multimédia peuvent être subdivisés en spams de messagerie textuelle et spams de messagerie vocale/vidéo. Un spam de messagerie textuelle est un message court incluant un texte commercial ou sollicité. Il présente des caractéristiques analogues au spam de courrier électronique ou au spam de SMS mobile, étant donné qu'il se présente sous la forme de texte. Toutefois, pour ce type de spam, le coût d'envoi devrait être nettement moins élevé que le cas du spam de SMS mobile. Un spam de messagerie vocale/vidéo est un message vocal/vidéo incluant un contenu commercial ou sollicité. Ce type de spam devrait gagner du terrain avec l'augmentation de l'utilisation d'applications multimédias IP. On prévoit que les messages vocaux/vidéo vont occuper une grande partie de la boîte de messagerie vocale/vidéo des utilisateurs d'applications IP ou des zones de stockage des fournisseurs de service IP, étant donné qu'un message multimédia a une taille beaucoup plus grande qu'un message de texte. Des spams multimédias peuvent aussi être utilisés pour transmettre des logiciels malveillants (vers, virus informatiques, logiciels espions, chevaux de Troie, etc.).

### **6.3 Spam de messagerie instantanée**

Le spam de messagerie instantanée, ou SPIM, est un autre type de spam d'application multimédia IP pouvant être gênant pour les utilisateurs d'un service de messagerie instantanée ciblés. Un grand nombre d'utilisateurs ont recours à la messagerie instantanée pour des raisons de commodité des communications avec les autres utilisateurs. Les spams de messagerie instantanée sont généralement des messages courts de type texte et ont de nombreux points communs avec les spams de courrier électronique, à ceci près que les spams de messagerie instantanée sont des messages en temps réel et peuvent être plus gênants. Les spams de messagerie instantanée peuvent aussi être des messages multimédias, étant donné que les services de messagerie instantanée prennent en charge de nombreuses fonctions en plus de la transmission de messages de texte en temps réel.

Il peut être difficile d'envoyer des spams de messagerie instantanée sans manipulation technique illégale, car la plupart des services de messagerie instantanée adoptent des listes de contacts basées sur des permissions, seuls les utilisateurs de ces listes étant autorisés à envoyer des messages. Toutefois, si le système de sécurité d'un service de messagerie instantanée présente des vulnérabilités, des spammeurs pourront peut-être dérober une liste de contacts ou une liste blanche d'un utilisateur cible et envoyer des spams en se faisant passer pour un membre de la liste de contacts.

Seuls les utilisateurs des listes de contacts peuvent envoyer des messages, mais n'importe qui peut demander la permission d'être ajouté sur une telle liste. Dans de nombreux services de messagerie instantanée, les messages de demande peuvent contenir quelques phrases de présentation du demandeur pour que l'utilisateur du service de messagerie instantanée dispose de renseignements sur le demandeur pour déterminer s'il permet ou non au demandeur d'être ajouté sur sa liste de contacts. Un spammeur ne figurant pas sur cette liste peut envoyer des spams en utilisant cette fonction du service de messagerie instantanée.

### **6.4 Spam de bavardage**

Des spams de bavardage peuvent être rencontrés dans divers types d'applications multimédias IP qui offrent des fonctions de bavardage entre les utilisateurs de service. La fonction de bavardage et la fonction de messagerie sont offertes dans de nombreuses applications multimédias IP (services de bavardage en ligne, services de jeux en ligne, etc.). Le spam de bavardage est généralement un message de texte court envoyé de façon répétée à tous les participants au bavardage. Par conséquent, certains services de bavardage en ligne et services de jeux en ligne limitent le nombre de transmissions du même message pour éviter les nombreuses transmissions d'un spam. Toutefois, l'effet de cette méthode est limité et d'autres mesures de lutte contre les divers types de spam de bavardage sont nécessaires.

Le service de bavardage présente les mêmes caractéristiques que le service de messagerie instantanée mais les types de spam que l'on peut rencontrer dans ces deux services sont différents. Un utilisateur de service de messagerie instantanée communique généralement avec les correspondants d'une liste de contacts qu'il a autorisés, de sorte qu'un spammeur doit entrer sur cette liste pour pouvoir envoyer des spams. Le service de bavardage est un service en ligne dans lequel les participants aux communications sont généralement inconnus. N'importe qui peut participer à un service de bavardage, en particulier des spammeurs, qui envoient généralement le même spam de façon répétée. Il est donc beaucoup plus simple d'envoyer des spams dans un service de bavardage que dans un service de messagerie instantanée.

### **6.5 Spam multimodal**

Le problème de sécurité lié aux spams se pose aussi dans le cas des interactions multimodales. Dans ce cas, un même spam multimédia peut atteindre plusieurs cibles sur une interface d'utilisateur et prendre une forme différente suivant la modalité. Par exemple, un spam sur le réseau peut prendre la forme d'un clip audio, d'un clip vidéo ou d'un message de texte sur l'écran, le contenu étant

identique ou différent. En tant que telles, les multimodalités augmentent l'exposition aux spams multimédias et on peut donc s'attendre à ce que le problème du spam multimodal s'amplifie lorsque les interactions multimodales se généraliseront.

## **6.6 Spam de service de partage de fichier de type P2P**

On peut aussi rencontrer des spams d'application multimédia IP de type P2P visant les utilisateurs de services de type P2P, par exemple le service de partage de fichier P2P. Les personnes raccordées à des réseaux IP peuvent utiliser un logiciel P2P pour partager entre elles divers types de fichiers informatiques. Ainsi, des spammeurs peuvent amener d'autres utilisateurs à télécharger des fichiers de spam en leur donnant le nom d'un film connu, d'une chanson connue, etc. Les spammeurs n'ont pas besoin de trouver de cibles. Ils ont simplement à offrir leurs fichiers de spam en partage pour que les autres utilisateurs du service P2P y accèdent. De nombreux fichiers de spam téléchargés devraient être exécutés, les destinataires de ces fichiers les téléchargent volontairement. Les dégâts causés par un spam dans un service P2P peuvent donc être considérables lorsque le spam contient un logiciel malveillant (ver ou virus par exemple) et non un contenu commercial.

## **6.7 Spam de site web**

Les spammeurs peuvent poster des articles ou des fichiers avec un contenu commercial sur de nombreux sites web aux finalités diverses. Un spam posté sur un babillard électronique peut être vu par un grand nombre de visiteurs du site web. Par exemple, des réponses avec un contenu commercial pour de nombreux articles de portails web et des articles commerciaux sur des blogs peuvent être des spams de site web. En plus des articles de type texte, les spammeurs peuvent aussi placer des fichiers audio et vidéo commerciaux sur des sites de partage audio/vidéo (par exemple un contenu UCC ou UGC) ou sur des babillards électroniques pour que les autres utilisateurs de service consultent ces fichiers. Un grand nombre d'utilisateurs de service de site web peuvent consulter les spams de site web, de sorte que, pour ce type de spam, les spammeurs n'ont pas besoin d'établir une liste de cibles pour envoyer des spams en masse.

## **7 Classification des spams multimédias IP**

Les spams d'application multimédia IP sont classés en deux groupes en fonction de leurs caractéristiques. Les spams d'application multimédia IP peuvent être classés en fonction de divers critères, par exemple le type d'application multimédia IP dans laquelle ils sont rencontrés, le type de média utilisé pour les envoyer, le protocole utilisé pour fournir le service, le type de message de protocole, etc. Dans le présent paragraphe, les spams multimédias IP sont classés en fonction des caractéristiques suivantes des applications multimédias IP, étant entendu que des techniques antisпам peuvent être appliquées en fonction de ces caractéristiques.

- spams multimédias IP en temps réel ou pas en temps réel: les services d'application multimédia IP peuvent être classés en fonction du critère de temps réel;
- type de média des spams multimédias IP: un service d'application multimédia IP peut prendre en charge des données textuelles, vocales, vidéo, ou une combinaison de ces données. Les données vidéo incluent les images fixes et les images animées.

Dans les services d'application multimédia IP en temps réel, l'établissement de la communication, la remise du message et la consultation du message par le destinataire ont lieu en temps réel. Le service de VoIP et le service de messagerie instantanée sont des exemples types d'applications multimédias IP en temps réel. Dans les services d'application multimédia IP pas en temps réel, le destinataire peut consulter ses messages quand il le souhaite. Les services web, le service P2P et les services de jeux en ligne sont des exemples d'applications multimédias IP pas en temps réel. La classification des spams d'application multimédia IP et des exemples représentatifs sont présentés dans le Tableau 7-1.

**Tableau 7-1 – Classification des spams d'application multimédia IP**

	<b>Texte</b>	<b>Voix</b>	<b>Vidéo</b>
En temps réel	<ul style="list-style-type: none"> <li>spam de messagerie instantanée</li> <li>spam de bavardage</li> </ul>	<ul style="list-style-type: none"> <li>spam de VoIP</li> <li>spam de messagerie instantanée</li> </ul>	<ul style="list-style-type: none"> <li>spam de messagerie instantanée</li> </ul>
Pas en temps réel	<ul style="list-style-type: none"> <li>spam de messagerie multimédia/textuelle</li> <li>spam textuel de service de partage de fichier P2P</li> <li>spam textuel de site web</li> </ul>	<ul style="list-style-type: none"> <li>spam de messagerie multimédia/vocale</li> <li>spam vocal de service de partage de fichier P2P</li> <li>spam vocal de site web</li> </ul>	<ul style="list-style-type: none"> <li>spam de messagerie multimédia/vidéo</li> <li>spam vidéo de service de partage de fichier P2P</li> <li>spam vidéo de site web</li> </ul>

## 7.1 Spam vocal en temps réel

Le spam vocal en temps réel peut être défini comme une communication vocale en temps réel non sollicitée dont l'objet est de faire la publicité d'un produit ou d'un service commercial, par exemple le spam de VoIP. Les spams vocaux en temps réel sont peut-être moins fréquents que les spams de courrier électronique mais on estime que le préjudice pour l'utilisateur de service est beaucoup plus grand. Un spam vocal en temps réel est très gênant pour son destinataire. Dans le service de courrier électronique, les utilisateurs peuvent consulter leurs courriers électroniques quand ils le souhaitent, peuvent identifier rapidement les spams et la suppression des spams leur demande relativement peu d'efforts. En revanche, les spams vocaux en temps réel sont plus intrusifs, étant donné qu'ils nécessitent une réponse immédiate de leurs destinataires. De plus, il faut plus de temps avant de se rendre compte que le message reçu est un spam vocal. Le spam vocal en temps réel est plus efficace que le spam de courrier électronique ou de SMS mobile. D'une manière générale, les spammeurs cherchent à persuader le destinataire du spam d'acheter un produit ou un service particulier. Dans le cas du spam vocal en temps réel, les télévendeurs cherchent à persuader le destinataire du spam par le biais d'une communication interactive, ce qui est plus invasif qu'un spam de courrier électronique ou de SMS, qui permet uniquement de transmettre un texte court ou une vidéo de façon non interactive. Plus le taux de persuasion est élevé, plus le préjudice causé par le spam est important. Ainsi, le préjudice causé par les spams vocaux en temps réel peut être relativement important compte tenu de la quantité de spams.

Les spammeurs peuvent essayer d'améliorer l'efficacité des spams vocaux en temps réel en utilisant divers services IP complémentaires, en plus des communications vocales de base. Les spams vocaux en temps réel sont généralement transmis aux destinataires par le biais de terminaux qui prennent en charge un service de VoIP. Un grand nombre de terminaux de ce type prennent en charge de nombreuses fonctionnalités comme la messagerie multimédia, la visiophonie et le partage d'écran, en plus des communications vocales qui constituent la fonction par défaut. Les spammeurs peuvent essayer de renforcer l'effet du spam en combinant le spam vocal en temps réel avec des services additionnels de type vidéo ou textuel.

Un spam vocal en temps réel peut être un spam illégal ou frauduleux avec une intention malveillante comme on peut aussi en rencontrer dans les services traditionnels de téléphonie filaire ou mobile. De plus, compte tenu du coût modique de la VoIP, ces spams illégaux de VoIP seront peut-être plus nombreux que les spams utilisant les services téléphoniques traditionnels. Par exemple, des spammeurs malveillants peuvent essayer d'accéder à des informations financières en envoyant des hameçons vocaux (vishing), pour obtenir de façon illégale des informations sur les utilisateurs de service. Des spammeurs malveillants peuvent envoyer des spams d'appât pour amener les destinataires de ces spams à utiliser un service très onéreux à leur insu. Par exemple, des spammeurs peuvent utiliser une 'machine automatique à sonnerie unique'. Cette machine établit une connexion avec un destinataire et met fin à l'appel après une ou deux sonneries ou procède rapidement à une déconnexion après avoir prononcé un petit mot comme "Allo". De nombreux

destinataires sont alors tentés de rappeler en utilisant l'information d'identification de l'appelant et sont alors raccordés à un système automatique de publicité ou à un service très onéreux. Ce type de spams est intéressant pour les spammeurs car le coût de l'envoi de ces spams est très modique. Des spams d'appât peuvent être envoyés par des spammeurs malveillants qui utilisent de façon abusive les vulnérabilités de sécurité des systèmes de VoIP. Par exemple, des spammeurs peuvent usurper des identités en détournant une session d'appel de VoIP. Un spammeur peut amener un utilisateur de service de VoIP à se raccorder au spammeur par usurpation d'identité lorsque l'utilisateur souhaite communiquer avec d'autres utilisateurs du service. De même, divers types de spams d'appât peuvent être rencontrés dans des applications multimédias IP.

## **7.2 Spam textuel en temps réel**

Le spam textuel en temps réel peut être défini comme un message textuel en temps réel de masse non sollicité, par exemple dans le but de faire la publicité d'un produit ou d'un service commercial. On peut rencontrer des spams textuels en temps réel dans de nombreuses applications multimédias IP qui assurent une transmission de message textuel en temps réel entre les utilisateurs de service. Le spam textuel en temps réel présente des caractéristiques analogues à celles du spam de courrier électronique étant donné qu'il est de type texte mais il est plus gênant car au moment où il arrive, son destinataire est interrompu. Le spam de messagerie instantanée et le spam de bavardage sont des exemples de spam textuel en temps réel.

Dans un grand nombre de services d'application multimédia IP (service de messagerie instantanée, service de bavardage en ligne, jeux en ligne, etc.), la fonction de transmission de message est offerte aux utilisateurs gratuitement ou à un prix très modique. Les spammeurs peuvent donc envoyer des spams textuels pour un coût très bas. Ils peuvent souvent obtenir des informations générales ou particulières sur les utilisateurs de service par diverses méthodes, ce qui leur permet de cibler davantage les destinataires et de tirer un meilleur profit de ces spams que des spams de courrier électronique, qui sont envoyés à des personnes non déterminées.

## **7.3 Spam vidéo en temps réel**

Le spam vidéo en temps réel peut être défini comme une communication vidéo en temps réel non sollicitée dont l'objet est de faire la publicité d'un produit ou d'un service commercial. Les données vidéo peuvent être des images fixes ou des images animées. On peut rencontrer des spams vidéo en temps réel dans des services d'application multimédia IP qui offrent une fonction de télécommunication vidéo en temps réel entre utilisateurs.

Dans un premier temps, les spams de type textuel ou vocal, qui peuvent être conçus sans difficulté considérable et dont le coût de transmission est bas, ne sont pas contraignants pour le réseau IP. Les spams vocaux en temps réel utilisés pour le télémarketing constituent une grande partie des spams d'application multimédia IP. Toutefois, à mesure que les technologies de partage et de transmission de média entre les utilisateurs de service d'application multimédia IP se développent et que la capacité du réseau augmente, les spams vidéo en temps réel peuvent rapidement gagner du terrain.

## **7.4 Spam vocal pas en temps réel**

Le spam vocal pas en temps réel peut être défini comme un message vocal de masse pas en temps réel et non sollicité dont l'objet est de faire la publicité d'un produit ou d'un service commercial. Le spam vocal enregistré est un exemple de spam vocal pas en temps réel.

Dans de nombreux cas, le service de VoIP prend en charge un service de messagerie multimédia, permettant d'envoyer et de recevoir des messages textuels, audio et vidéo, en plus de la fonction d'appel téléphonique en temps réel. Les spammeurs peuvent envoyer au terminal d'un destinataire un spam vocal déjà enregistré en utilisant cette fonction du service de VoIP. Ce type de spam vocal est très gênant pour les utilisateurs et les fournisseurs de service de VoIP car il a une grande taille et

occupe une grande place dans la boîte de messagerie vocale ou dans la zone de stockage des messages vocaux.

### **7.5 Spam textuel pas en temps réel**

Le spam textuel pas en temps réel peut être défini comme un message textuel de masse pas en temps réel et non sollicité, par exemple dans le but de faire la publicité d'un produit ou d'un service commercial. Le spam textuel pas en temps réel présente des caractéristiques analogues à celles du spam de courrier électronique. On peut rencontrer des spams textuels pas en temps réel dans diverses applications multimédias IP, étant donné qu'il n'est pas difficile de créer et de transmettre des messages textuels et que le coût d'envoi de ce type de spam est généralement modique.

Des spams textuels pas en temps réel peuvent être envoyés à des terminaux IP, qui peuvent recevoir des messages textuels longs tels que les courriers électroniques, ou à des téléphones VoIP, qui peuvent recevoir des messages textuels courts tels que des SMS mobiles. On peut rencontrer ce type de spams dans un grand nombre de services d'application multimédia IP dont la messagerie instantanée et divers services en ligne. En plus des types de spams textuels qui sont envoyés à des destinataires à leur insu, il existe d'autres types de spams textuels auxquels les utilisateurs de service IP sont exposés, par exemple les publicités postées sur les sites web. Le spam textuel pas en temps réel présente des caractéristiques analogues à celle du spam de courrier électronique et de nombreuses techniques de lutte contre le spam de courrier électronique devraient lui être appliquées. L'applicabilité de ces techniques pourra être limitée lorsque le spam textuel est court.

### **7.6 Spam vidéo pas en temps réel**

Le spam vidéo pas en temps réel peut être défini comme un message vidéo de masse pas en temps réel et non sollicité, par exemple dans le but de faire la publicité d'un produit ou d'un service commercial. Il peut être de l'un des deux types suivants: les utilisateurs d'un service IP obtiennent ou téléchargent un fichier de spam vidéo, ou bien ils accèdent à un spam vidéo sous la forme d'une vidéo à la demande à partir de services d'application multimédia IP. Les méthodes de transmission du spam vidéo pas en temps réel sont de deux types. Dans le premier cas, un destinataire peut obtenir à son insu un fichier publicitaire vidéo envoyé par un spammeur. Dans l'autre cas, un utilisateur de service d'application multimédia IP télécharge un fichier de spam par le biais d'un service de partage de fichier en ne se doutant pas qu'il s'agit d'un fichier de spam.

Un destinataire qui télécharge un fichier de spam vidéo perd du temps et de l'énergie. La transmission de spams vidéo à des destinataires à leur insu cause des préjudices aux utilisateurs et aux fournisseurs de service car ces messages vidéo sont généralement de grande taille et occupent une grande place dans la boîte de messagerie ou dans la zone de stockage.

## **8 Aspects techniques liés à la lutte contre le spam multimédia IP**

Comme dans le cas du spam de courrier électronique ou de SMS mobile, on donne ci-après une série de procédures relatives à la création, à l'envoi et à la prévention des spams dans les services d'application multimédia IP:

- Création et transmission de spams.
- Détection et filtrage des spams par les utilisateurs et/ou les fournisseurs de service d'application multimédia IP.
- Mesures à prendre concernant les spams reçus.

Avant d'établir un cadre technique de lutte contre le spam d'application multimédia IP, il faut étudier les faiblesses de la prévention de ce type de spam dans les différentes procédures mentionnées ci-dessus. Compte tenu des vulnérabilités, il convient de prendre en considération le type d'aspects techniques à chaque étape de la lutte contre le spam d'application multimédia IP. Une analyse de l'incidence que ces aspects peuvent avoir sur la création et la transmission de spams

multimédias IP est présentée ci-dessous. Lors de l'étude du cadre technique et des moyens techniques de lutte contre le spam multimédia IP, l'analyse contenue dans le présent paragraphe pourra être utile pour déterminer comment lutter efficacement contre ce type de spam.

## **8.1 Création et transmission de spams**

Pour que les spams multimédias IP se généralisent, il faut que le coût d'envoi de ces spams soit faible par rapport au profit que le spammeur s'attend à en retirer. Ce coût inclut non seulement un coût monétaire mais aussi divers types de ressources en termes de temps et d'efforts ainsi que la difficulté technique rencontrée pour pouvoir créer et transmettre des spams multimédias IP. Les facteurs qui ont une incidence sur le coût de l'envoi de spams sont les suivants:

- coût de collecte d'adresses cibles ou de numéros de téléphone cibles: coût nécessaire pour collecter les adresses et numéros de téléphone des cibles des spams;
- coût de création et de transmission des spams: coût nécessaire pour créer et transmettre des spams pour le spammeur.

### **8.1.1 Etablissement d'une liste de cibles**

Avant d'envoyer des spams, il faut commencer par établir des listes de cibles. Les spammeurs peuvent obtenir sans grande difficulté des liste de cibles de spams de courrier électronique au moyen d'attaques de type dictionnaire ou de programmes de collecte d'adresses de courrier électronique ou en accédant illégalement à des listes établies de cibles. Dans le cas du spam de SMS mobile, de simples combinaisons de numéros permettent d'établir des listes de cibles, étant donné que l'ensemble des numéros de téléphone mobile est limité.

Le type d'identificateur de personne spécifique utilisé pour les communications et les échanges de messages entre utilisateurs de service d'application multimédia IP peut varier en fonction du type d'application multimédia IP, du protocole, de la réglementation nationale, etc. Les identificateurs de personne qui peuvent être utilisés pour le service de VoIP peuvent prendre la forme de numéros de téléphone (comme pour le service de RTPC), d'adresses IP, de comptes de service IP (par exemple des comptes de courrier électronique), etc. Pour le service de messagerie instantanée, on utilise généralement l'adresse de courrier électronique comme identificateur de personne, d'autres types d'information comme le numéro de téléphone mobile pouvant aussi être utilisés.

Lorsque ces types d'identificateurs de personne sont utilisés pour la VoIP et la messagerie instantanée, les spammeurs peuvent collecter les identificateurs de personne et les comptes du service correspondant à ces services en utilisant les méthodes d'établissement de liste de cibles utilisées pour les spams de courrier électronique. Des adresses d'utilisateur de VoIP et de messagerie instantanée devraient être collectées sans grande difficulté au moyen d'une attaque de type dictionnaire, d'un programme de collecte d'identificateurs utilisant une recherche sur le réseau, etc.

Outre la VoIP et la messagerie instantanée, il existe divers types d'applications multimédias IP dans lesquelles on peut rencontrer des spams: services de bavardage, services de jeux en ligne, services de type P2P, etc. Il semble que l'établissement de listes de cibles de spams pour ces applications multimédias IP ne nécessite pas non plus de gros efforts. Un grand nombre de ces applications multimédias IP (par exemple les services en ligne) utilisent des types de comptes très courants, par exemple des adresses de courrier électronique et des numéros de téléphone, comme identificateurs de personne. Il n'est généralement pas difficile d'accéder à la liste des utilisateurs d'un service d'application multimédia IP pour lequel seuls les utilisateurs acceptés sont autorisés à transmettre des fichiers ou des messages. Ainsi, si aucune mesure particulière n'est prise pour compliquer la collecte d'identificateurs des utilisateurs de service d'application multimédia IP, il n'est pas difficile pour les spammeurs d'établir une liste de cibles aussi bien du point de vue technique que du point de vue économique.

### **8.1.2 Création et transmission de spams**

Le coût nécessaire pour créer et transmettre des spams d'application multimédia IP devrait représenter la plus grande partie des coûts liés à l'envoi de spams multimédias IP. Le coût du service de VoIP ou des communications vocales dans divers types d'applications multimédias IP est généralement moins élevé que le coût du service de téléphonie filaire à commutation de circuits ou du service de téléphonie mobile. Pour les spammeurs qui utilisaient les services traditionnels de téléphonie filaire ou sans fil pour faire du télémarketing actif, la VoIP ou les communications vocales dans des applications multimédias IP constituent des services intéressants pour la transmission de spams. De plus, les appels longue distance et les appels internationaux sont nettement meilleur marché que dans le cas des services téléphoniques traditionnels. Ainsi, les spams de télémarketing peuvent s'étendre à d'autres pays qui utilisent la même langue et peuvent provenir d'autres pays dans lesquels le coût d'un télévendeur et le coût de transmission des spams sont très bas.

Outre le service de VoIP, de nombreuses applications multimédias IP comme la messagerie instantanée, le service de type P2P et les services de bavardage en ligne sont offertes gratuitement ou à un prix très modique. La création et la transmission de spams dans ces applications ne devrait pas représenter beaucoup d'efforts ni un coût élevé, étant donné qu'en règle générale, elles sont peu onéreuses, prennent peu de temps et présentent peu de difficultés techniques.

### **8.2 Détection et filtrage des spams**

La détection et le filtrage des spams d'application multimédia IP constituent l'élément technique le plus important pour lutter efficacement contre ces spams. Il est possible de filtrer les spams de courrier électronique au niveau du serveur de l'ISP ou de l'intranet ou du terminal d'un destinataire de courrier électronique avant que le destinataire ne les consulte, car le service de courrier électronique fonctionne selon le mécanisme d'enregistrement et retransmission des communications. Une partie des spams de courrier électronique peuvent être filtrés par l'application en utilisant diverses techniques de filtrage (analyse de contenu, etc.), car la plupart des courriers électroniques ont un contenu de type texte. Contrairement aux spams de courrier électronique, on estime qu'il est difficile de filtrer les spams multimédias IP en raison des caractéristiques suivantes des applications multimédias IP:

- communications en temps réel;
- difficulté d'analyse du contenu vocal et vidéo;
- difficulté d'authentification des spammeurs.

Certaines applications multimédias IP comme la VoIP et la messagerie instantanée assurent des communications en temps réel entre les utilisateurs de service. Dans ces applications, les spams sont transmis en temps réel aux destinataires sans être enregistrés au niveau d'un serveur. Dans certains cas, le contenu de VoIP et de messagerie instantanée ne passe pas par les serveurs des fournisseurs de service mais est transmis directement à l'utilisateur de service. Il est donc difficile d'obtenir des informations suffisantes au sujet de la communication et d'analyser son contenu pour déterminer s'il s'agit d'un spam avant que l'appel ne soit établi ou que le message ne soit transmis. Par exemple, lorsqu'un message a été envoyé par un expéditeur à un destinataire et que le destinataire se rend compte qu'il s'agit d'un spam, il est trop tard pour filtrer le spam, étant donné que la communication est déjà terminée. Dans le cas du spam de messagerie instantanée, il peut être possible d'analyser le contenu du message instantané pendant une très courte période, étant donné que les messages instantanés sont généralement de type texte. Toutefois, la brièveté des messages instantanés peut réduire l'efficacité des techniques de filtrage traditionnelles mises au point pour lutter contre le spam de courrier électronique. Il appartient aux terminaux des utilisateurs de service de filtrer les spams lorsque le contenu des applications multimédias IP ne passe pas par le serveur de l'ISP. Mais l'ajout d'un filtrage des spams dans les terminaux des utilisateurs de service et la gestion de la fonction de filtrage des spams par les utilisateurs ne sont pas simples. Par conséquent, il ne sera

peut-être pas possible de détecter et de filtrer des spams d'application multimédia IP en temps réel (spam de VoIP et spam de messagerie instantanée par exemple) au moyen d'une analyse de contenu.

On pourra adopter des mécanismes d'enregistrement et retransmission des communications pour certaines applications multimédias IP qui n'ont pas besoin d'être en temps réel (messagerie multimédia par exemple). La transmission de fichiers par la technique P2P peut être une technique pour lutter contre le spam au moyen d'une analyse de contenu lorsque les fournisseurs ou les utilisateurs de service le demandent. Toutefois, il reste difficile de détecter et de filtrer les spams au moyen d'une analyse de contenu, car la technologie de reconnaissance vocale et vidéo n'est pas encore au point et l'application de cette technologie pourra occasionner une charge importante dans le réseau.

On peut aussi identifier les spams sur la base d'informations relatives à l'expéditeur, et non sur la base du contenu. Il est possible de déterminer si l'expéditeur est un spammeur ou non en utilisant diverses techniques (listes noires, listes blanches, systèmes de réputation, etc.). L'application de ces techniques aux spams d'application multimédia IP présente plusieurs points faibles. Tout d'abord, il n'est pas difficile d'établir des comptes de service ou des identificateurs de personne pour les applications multimédias IP et un grand nombre peuvent être établis. Les spammeurs peuvent facilement établir un nouvel identificateur lorsque leur ancien identificateur est classé dans la catégorie des spammeurs. Ils peuvent également se faire passer pour des utilisateurs de service normaux en exploitant les vulnérabilités de sécurité des applications multimédias IP. Cela étant, il est nécessaire de combiner des techniques antispam qui identifient les spams sur la base d'informations relatives à l'expéditeur avec des mécanismes d'authentification efficaces.

### **8.3 Mesures à prendre concernant les spams reçus**

Un destinataire peut prendre plusieurs mesures après avoir reçu un spam. Il peut ajouter l'identificateur du spammeur sur une liste noire pour éviter que ledit spammeur ne lui envoie d'autres spams ou en envoie à d'autres utilisateurs. Il peut aussi donner une mauvaise note au spammeur dans des systèmes de réputation. Il est également possible de signaler un spam illégal afin de sanctionner le spammeur. Toutefois, comme indiqué précédemment, il est difficile d'identifier les spammeurs dans de nombreuses applications multimédias IP et il est facile de créer un nouvel identificateur. A ce stade, il est également nécessaire d'adopter un mécanisme d'authentification efficace afin d'augmenter l'efficacité des mesures prises concernant les spams reçus.

## **9 Menaces de sécurité liées au spam**

Le présent paragraphe porte sur des aspects de sécurité liés aux spams multimédias IP. Certaines menaces de sécurité sont définies et classées par catégories et des contremesures sont décrites.

### **9.1 Menaces de sécurité liées au spam**

Le présent paragraphe porte sur certaines menaces de sécurité que l'on peut rencontrer dans les applications multimédias IP. Les menaces de sécurité sont définies du point de vue de l'envoi de spams dans le réseau. Pour envoyer des spams, un spammeur peut utiliser les techniques d'attaque suivantes dans les environnements multimédias IP.

#### **9.1.1 Collecte d'identificateurs**

Avant d'envoyer des spams, le spammeur collecte des identificateurs pour trouver des cibles pour ses spams. La collecte d'identificateurs, qui est un processus préliminaire essentiel, constitue donc la menace la plus courante. Le spammeur essaie de collecter le plus grand nombre possible d'identificateurs, car le nombre d'identificateurs correspond au nombre de cibles à attaquer du point de vue du spammeur. Les identificateurs peuvent être collectés par divers moyens: moteurs de recherche, forums libres, etc. Des identificateurs peuvent être créés avec des mots généraux et des

noms. Parfois, des identifiants peuvent être collectés à partir de transactions illégales avec des entreprises ou des écoles qui peuvent avoir de nombreux clients présentant des informations personnelles.

Dans de nombreuses applications multimédias IP, des identifiants uniques (par exemple des adresses de courrier électronique et des identifiants URI) ont été utilisés pour faire la distinction entre les différents utilisateurs. A la différence du service téléphonique, les services d'application multimédia IP présentent plusieurs avantages tels que des télécommunications multicanal, un bas prix, etc., ce qui explique que les environnements multimédias IP soient particulièrement prisés par les spammeurs. Par conséquent, les utilisateurs devraient veiller à protéger leurs identifiants et à ne pas les laisser exposés aux spammeurs.

### **9.1.2 Usurpation d'identité d'expéditeur**

L'usurpation d'identité est un type de technique de piratage. Une personne malveillante peut construire un site web sur le réseau et amener d'autres personnes à visiter ce site pour obtenir leur autorité et leur dérober leurs informations personnelles en exploitant un défaut organisationnel de TCP/IP. De plus, si un spammeur envoie un spam en se faisant passer pour une société connue, le destinataire pourra penser que ce message provient d'un expéditeur digne de confiance. Ces spams ont une forte probabilité d'être acceptés. Dans ce cas, on parle également d'usurpation d'identité.

L'envoi de spams via usurpation d'identité d'expéditeur est une menace pour laquelle le spammeur se fait passer pour quelqu'un d'autre en falsifiant le champ d'en-tête de message ou l'identifiant d'expéditeur utilisé dans des applications multimédias IP. Cette menace peut altérer la liste blanche et la liste noire qui sont des solutions antispam bien connues. Par exemple, si un spammeur remplace son identifiant par celui d'un utilisateur valable qui est inscrit sur la liste blanche ou sur la liste de contacts du destinataire, il peut contourner la politique basée sur la liste blanche. En outre, compte tenu de la nature des communications multimédias, il est difficile de déterminer si le message est un spam ou non avant que la connexion ne soit établie. Par conséquent, dans ce cas, le destinataire n'a pas d'autre choix que de recevoir le spam.

### **9.1.3 Reniflage d'informations d'enregistrement**

Le reniflage est le comportement d'un spammeur qui écoute clandestinement les communications en cours entre d'autres utilisateurs. L'outil utilisé pour le reniflage est appelé renifleur.

Dans l'environnement multimédia IP, un spammeur peut envoyer des spams en utilisant de façon illégale un renifleur. Il commence par utiliser un renifleur pour obtenir les informations d'enregistrement d'un utilisateur valable pour certaines applications puis utilise ces informations pour générer de fausses informations d'enregistrement. Il insère ensuite l'adresse IP d'un attaquant au lieu de l'adresse IP de l'utilisateur valable dans le message d'enregistrement. Il peut alors envoyer des spams en utilisant le faux enregistrement.

### **9.1.4 Détournement de session**

Le détournement de session est une technique dans laquelle une personne détourne une session de communication entre d'autres utilisateurs. Cette technique peut être employée pour envoyer des spams dans des environnements multimédias IP. Un spammeur peut imposer une déconnexion entre deux utilisateurs au milieu de la session. Dans ce cas, les utilisateurs ont tendance à rétablir la session précédente. Le spammeur peut alors détourner la session et peut insérer une transmission de média RTP contenant un spam au milieu de la session rétablie.

### **9.1.5 Injection SQL**

L'injection SQL est une technique de piratage qui donne un résultat anormal dû à l'insertion d'une syntaxe de requête à l'insu du demandeur. Dans un environnement d'applications multimédias IP, l'injection SQL peut être utilisée lors de l'application d'un mécanisme HTTP Digest pour l'authentification. Le spammeur modifie l'en-tête d'authentification et insère une fausse requête

SQL. Il falsifie ensuite l'en-tête d'authentification du message dans le serveur proxy que le mécanisme HTTP Digest utilise pour l'authentification, et insère une fausse requête SQL. Si cette attaque se termine avec succès, le spammeur peut se faire passer pour un utilisateur authentifié et envoyer des spams avec une autorisation valable en falsifiant les informations d'enregistrement d'un utilisateur valable.

### **9.1.6 Robot de spam**

Un robot de spam est un robot malveillant se présentant sous la forme d'un programme ou d'un code qui peut être contrôlé et exploité à distance mais qui ne peut pas s'autoactiver. En règle générale, il est contrôlé via une connexion utilisant un protocole IRC. Un réseau de robots est appelé botnet. Un spammeur peut contrôler un grand nombre de systèmes infectés en utilisant une seule commande, car les botnets peuvent être reliés. Un spammeur peut donc envoyer facilement une grande quantité de spams en utilisant cette technique dans des applications multimédias IP.

### **9.1.7 Empoisonnement de cache**

L'empoisonnement de cache est une attaque qui consiste à remplacer des adresses de domaine par d'autres adresses, qui sont erronées. Cette technique peut être utilisée dans les protocoles ARP et NDP dans des applications multimédias IP. Le protocole ARP sert à faire correspondre les adresses IP et MAC dans les réseaux IPv4 et le protocole NDP sert à découvrir les nœuds voisins dans les réseaux IPv6. Les paquets ARP et NDP sont retransmis à tous les dispositifs qui sont connectés sur une même liaison. Les spammeurs peuvent recourir à la méthode de l'empoisonnement de cache pour modifier le contenu du cache ARP ou du cache NDP en interceptant des paquets.

Par exemple, un spammeur peut se faire passer pour une passerelle en utilisant l'empoisonnement de cache ARP et intercepter tous les paquets sur la liaison correspondante. Ainsi, si un utilisateur lance une connexion, le spammeur peut insérer un spam RTP préparé dans la session en cours et peut modifier l'identificateur du destinataire, auquel cas l'utilisateur pourra essayer d'établir une autre connexion avec l'utilisateur dont l'identificateur a été indiqué par le spammeur, mais qui n'est pas l'utilisateur de départ. Avec cette attaque, le spammeur pourra envoyer un spam à l'utilisateur qui demande la connexion.

### **9.1.8 Contrôle du routage**

On suppose qu'une communication pour des applications multimédias IP est en cours entre des routeurs et des utilisateurs et qu'un spammeur joue un rôle de routage dans la communication à l'intérieur d'un réseau via un piratage. Si un utilisateur essaie d'établir des connexions avec d'autres utilisateurs appartenant à ce réseau particulier, le spammeur répond à la demande en se faisant passer pour un utilisateur valable et envoie un spam à l'utilisateur qui a demandé la connexion.

### **9.1.9 Système de gestion vulnérable**

Il existe un autre type de menace, qui repose sur les vulnérabilités du système de gestion de service. Dans ce cas, un spammeur peut modifier les informations d'enregistrement d'un utilisateur valable et envoyer un spam avec les caractéristiques de l'utilisateur valable.

## **9.2 Classification des menaces de sécurité liées aux spams**

Les menaces de sécurité liées au spam mentionnées ci-dessus peuvent être classées par technique d'attaque. Cette classification est présentée dans le Tableau 9-1.

**Tableau 9-1 – Menaces de sécurité liées au spam classées par technique d'attaque**

Technique d'attaque	Menaces de sécurité liées au spam
code malveillant/contrôle à distance	robot de spam
détournement de session	détournement de session
injection SQL	injection SQL
reniflage	reniflage d'informations d'enregistrement
usurpation d'identité	usurpation d'identité d'expéditeur, empoisonnement de cache, contrôle du routage
autres	collecte d'identifiants, système de gestion vulnérable

La technique du code malveillant/contrôle à distance permet de transmettre facilement une grande quantité de spams. Un spammeur peut distribuer des codes malveillants par divers moyens et contrôler les machines infectées pour envoyer des spams. Les robots de spam sont un exemple.

Le détournement de session est une technique de piratage qui consiste à dérober une session à quelqu'un. En règle générale, il suffit de deviner l'identifiant de session et d'utiliser un cookie de cet identifiant. Un spammeur peut écouter clandestinement la communication entre un serveur et un utilisateur sans procédure d'authentification ou avec l'autorisation du serveur.

L'injection SQL est une méthode de piratage qui exploite une vulnérabilité de bases de données. Cette méthode consiste à modifier la requête SQL normale et à procéder à une authentification, de façon illégale. Elle est généralement utilisée dans le piratage des sites web pour dérober des informations relatives aux utilisateurs.

Le reniflage est une technique dans laquelle un pirate observe les paquets échangés entre deux utilisateurs ou plus.

L'usurpation d'identité est une technique dans laquelle une personne se fait passer pour une autre personne. Un utilisateur peut alors croire que le spammeur avec lequel il communique est une personne digne de confiance.

### 9.3 Contremesures

Pour résoudre le problème du spam décrit ci-dessus, on dispose de trois contremesures: l'authentification, l'autorisation et la gestion de la sécurité. Par gestion de la sécurité, on entend la contremesure qui peut être appliquée à une configuration de sécurité appropriée en installant un correctif de sécurité dans des systèmes conçus pour assurer la maintenance et la réparation et pour sensibiliser davantage l'utilisateur en matière de sécurité. Il existe diverses contremesures comme le contrôle de flux, le chiffrement, etc., auxquelles on peut s'intéresser. Le présent paragraphe porte sur les trois principales contremesures.

Les relations entre les contremesures et les menaces de sécurité liées aux spams sont présentées dans le Tableau 9-2.

**Tableau 9-2 – Relations entre les contremesures et les menaces de sécurité liées aux spams de communication multimédia**

Menaces \ Contremesures	Authentification	Autorisation	Gestion de la sécurité
Collecte d'identifiants			X
Usurpation d'identité d'expéditeur	X		
Reniflage d'informations d'enregistrement	X		
Détournement de session	X		
Injection SQL		X	X
Robot de spam			X
Empoisonnement de cache	X		
Contrôle du routage	X		
Système de gestion vulnérable		X	X

L'authentification permet de remédier à de nombreuses menaces de sécurité liées aux spams en résolvant les problèmes d'usurpation d'identité. L'usurpation d'identité est utilisée dans divers cas: usurpation d'identité d'expéditeur, reniflage d'informations d'enregistrement, détournement de session, empoisonnement de cache, contrôle du routage, etc. Concernant l'usurpation d'identité d'expéditeur, chaque expéditeur est authentifié par un procédé d'authentification après la réception du message. Concernant les attaques par reniflage d'informations d'enregistrement, il est interdit à un utilisateur non authentifié de modifier les informations d'enregistrement lors de l'authentification. Concernant les attaques par détournement de session ou par empoisonnement de cache, les utilisateurs sont authentifiés avant de pouvoir participer aux communications. Concernant le contrôle du routage, seul un utilisateur authentifié peut contrôler un routeur.

Toutefois, il existe des cas où l'authentification ne permet pas de remédier aux menaces de sécurité liées aux spams. Dans le cas de l'injection QSL, il faut établir une politique d'autorisation. Dans le cas des systèmes de gestion vulnérables, un gestionnaire du système devrait accorder différentes autorisations d'accès aux utilisateurs en fonction des comptes d'utilisateur.

Enfin, certaines menaces de sécurité liées aux spams nécessitent une gestion rigoureuse de la sécurité. Il s'agit notamment de la collecte d'identifiants, de l'injection SQL, du robot de spam et des systèmes de gestion vulnérables. Un spammeur peut collecter un identifiant d'utilisateur par de nombreux moyens et envoyer des spams. Une gestion rigoureuse des identifiants est donc nécessaire. Les développeurs de systèmes devraient en tenir compte lorsqu'ils développent des systèmes, car les menaces d'injection SQL sont parfois dues à un code défectueux. Un robot de spam est causé par une infection par un robot malveillant. Par conséquent, les utilisateurs d'ordinateur devraient faire attention lorsqu'ils téléchargent des fichiers ou accèdent à des sites web et devraient veiller à protéger leur système d'exploitation. Dans le cas des systèmes de gestion vulnérables, les gestionnaires de systèmes devraient gérer leurs systèmes avec soin.

## **10 Applicabilité de mécanismes connus de lutte contre le spam au cas des applications multimédias IP**

De nombreuses études ont été faites sur divers mécanismes pour lutter contre le spam classique de courrier électronique. Certaines des solutions utilisées pour le spam de courrier électronique peuvent aussi être employées pour lutter contre le spam multimédia IP. Avant de s'intéresser à l'ensemble des solutions concernant le spam multimédia IP, il est nécessaire d'analyser les mécanismes classiques de lutte contre le spam et d'examiner leur applicabilité dans le cas du spam

multimédia IP. Par conséquent, le présent paragraphe va examiner certains mécanismes connus de lutte contre le spam du point de vue de leur applicabilité dans le cas du spam multimédia IP.

## **10.1 Filtrage par identification**

### **10.1.1 Liste noire**

Une liste noire est une liste d'identifications (adresses de courrier électronique par exemple) qui sont suspectes ou identifiées comme étant celles de spammeurs. Le mécanisme d'une liste noire consiste à filtrer les messages ou les appels provenant d'expéditeurs inscrits sur cette liste. La liste noire peut comporter des adresses IP, des noms de domaine, des identifications ou adresses d'appelant, des contenus d'en-tête ou de corps, ou une combinaison de ces différents types, qui peuvent être utilisés pour faciliter l'identification des spams.

Le simple recours à une liste noire pour lutter contre le spam ne sera peut-être pas efficace dans les applications IP. Le spammeur peut utiliser l'identification d'une personne innocente et usurper l'identité d'un destinataire. Pour résoudre ce problème, on peut utiliser des mécanismes d'authentification fondés sur l'adresse d'origine. Un autre problème concernant cette méthode est qu'un utilisateur peut créer très facilement de nouvelles identifications. Diverses applications multimédias IP conçues pour les télécommunications utilisent des adresses de courrier électronique. Une adresse de courrier électronique peut facilement être créée sur divers sites portails connus. Un grand nombre d'abonnés n'envoyant pas de spam utilisent des adresses créées sur ces sites portails, de sorte que le nom de domaine des sites portails ne peut pas être inscrit sur liste noire. Pour résoudre ce problème, les fournisseurs de service de portail doivent ajouter une certaine complexité pour la création de nouvelles adresses. Si le temps et les efforts nécessaires pour créer une nouvelle adresse sont considérables, le spammeur finira par utiliser une autre méthode pour créer de nouvelles adresses pour l'envoi de spams, adresses qui auront alors de meilleures chances d'être filtrées par la méthode de la liste noire de domaine. La méthode de la liste noire devient donc efficace lorsqu'elle est combinée à d'autres méthodes.

La méthode de la liste noire n'est appliquée qu'une seule fois au début de la communication lorsqu'une identification de l'origine est rencontrée pour la première fois. Il est donc possible d'utiliser cette méthode pour tout type d'application multimédia IP qui utilise une identification telle qu'une adresse d'origine. Dans le cas des applications de site web, on peut utiliser cette méthode pour accorder le droit de poster un contenu uniquement aux utilisateurs non spammeurs, c'est-à-dire aux utilisateurs ne figurant pas sur la liste noire. On peut donc utiliser la méthode de la liste noire pour bloquer tous les types de spams multimédias IP qui utilisent un type quelconque d'identification qu'il s'agisse d'une application en temps réel ou non.

### **10.1.2 Liste blanche**

Une liste blanche est le contraire d'une liste noire: elle contient des informations relatives à des utilisateurs de confiance. Les courriers électroniques provenant d'expéditeurs inscrits sur la liste blanche seront toujours acceptés. Contrairement à une liste noire, la création massive d'adresses de courrier électronique pour changer d'identité ne facilite pas l'inscription sur la liste blanche, mais une usurpation d'adresse est toujours possible. Les spams reposant sur une usurpation d'adresse peuvent être filtrés facilement au moyen de méthodes d'authentification forte.

Même si la méthode de la liste blanche permet de filtrer la quasi-totalité des spams, une personne normale a parfois besoin de communiquer avec des personnes ne figurant pas sur la liste blanche. Si un expéditeur ne figurant pas sur la liste blanche d'un utilisateur a besoin de communiquer avec cet utilisateur, un certain type de méthode d'autorisation devra lui être appliquée avant qu'il ne puisse être inscrit sur cette liste blanche. L'utilisateur devra valider l'identification de l'expéditeur ou certains commentaires de présentation envoyés par l'expéditeur. L'utilisateur peut accepter ou refuser la demande de communication. Un expéditeur accepté peut être inscrit sur la liste blanche de l'utilisateur. Si l'utilisateur doit accepter ou refuser chaque nouvelle demande, cela sera très gênant

car la plupart des nouvelles demandes sont des spams. Un autre inconvénient de cette méthode est que l'utilisateur doit configurer la liste blanche lorsqu'il change d'environnement, ce qui constitue une perte de temps et d'énergie.

Le concept de listes blanches est déjà intégré dans les systèmes de messagerie instantanée sous le nom de liste de contacts. Les nombreux systèmes de messagerie instantanée autorisent uniquement les communications entre utilisateurs inscrits sur la liste de contacts et possèdent une capacité de type permission pour accepter l'ajout d'un nouvel utilisateur sur la liste de contacts. Ainsi, conjointement avec des mécanismes d'authentification forte, cette méthode peut s'avérer utile pour lutter contre le spam de messagerie instantanée. Toutefois, la VoIP présente des caractéristiques différentes des systèmes de messagerie instantanée. Comme dans le cas des systèmes de courrier électronique, les listes blanches peuvent s'avérer utiles en complément d'autres méthodes, car les utilisateurs ont tendance à toujours accepter les appels provenant d'appelants inconnus.

La méthode de la liste blanche est utilisée uniquement au début de la communication, elle est donc adaptée aux applications en temps réel ou non. Dans le cas des applications de site web, on peut utiliser cette méthode pour accorder le droit de poster un contenu uniquement aux utilisateurs inscrits sur la liste blanche.

### **10.1.3 Système de réputation**

Un système de réputation est utilisé conjointement avec une liste blanche ou noire. Si un expéditeur qui ne figure pas sur la liste noire ou sur la liste blanche d'un destinataire souhaite communiquer avec ce destinataire, une note de réputation est affichée sur le terminal du destinataire. Cette note aide le destinataire à décider s'il doit accepter ou refuser l'appel. Si l'utilisateur accepte la demande de communication et découvre que l'expéditeur est un spammeur, il peut envoyer un rapport de spam au système de réputation et l'identification de l'expéditeur n'est pas ajoutée sur la liste blanche de l'utilisateur. Les rapports, qui sont accumulés dans le serveur de réputation, donnent une note de réputation.

Un inconvénient de cette méthode est qu'un spammeur possédant une note de réputation négative peut changer d'identification et recommencer à envoyer des spams avec sa nouvelle identification. La nouvelle identification ne sera pas associée à une note négative et il faudra un certain temps avant que cet utilisateur accumule les notes négatives et soit considéré comme un spammeur. Un autre inconvénient est qu'un groupe de personnes malveillantes peuvent intimider une victime innocente en la menaçant de lui donner une note de réputation négative. Il sera alors difficile pour cette victime de poursuivre ses activités sur les réseaux IP.

Un autre type de système de réputation est le système de réputation positive. Le destinataire donne une note positive aux utilisateurs qui ne sont pas des spammeurs. Dans cette méthode, il est difficile d'envoyer des spams sous une nouvelle identification, car toute nouvelle identification est associée à une note relativement basse. Un inconvénient de cette méthode est que plusieurs spammeurs peuvent se rassembler et se donner des notes positives les uns aux autres. Mais pour cela, les spammeurs doivent former une sorte de consortium, ce qui coûte très cher. Le système de réputation positive est donc plus efficace que le système de réputation négative.

Pour que le système de réputation fonctionne, il faut un système de télécommunication à commande centralisée et monolithique. Cette méthode peut donner de bons résultats dans le cas des applications de messagerie instantanée, qui sont normalement exploitées par un seul fournisseur de service. En revanche, les applications de VoIP prennent en charge des communications entre divers fournisseurs de service. La note de réputation peut varier d'un fournisseur de service à l'autre, car il n'existe pas de définition normalisée. Par conséquent, cette méthode n'est pas adaptée pour les applications telles que la VoIP pour lesquelles il n'existe pas de système de description normalisé.

On peut aussi recourir au système de réputation dans les applications qui utilisent un certain type d'identification des expéditeurs, car la note de réputation peut être associée à l'identification. Si

l'expéditeur passe avec succès l'épreuve du système de réputation, il sera ajouté sur la liste blanche du destinataire. Cette méthode peut donc être utilisée dans toute application en temps réel ou non.

On peut aussi utiliser cette méthode dans les applications web pour accorder le droit de poster un contenu uniquement aux utilisateurs dont la note de réputation a dépassé un certain niveau. Le site web peut garder une note de réputation pour chaque membre en conservant la note donnée pour les activités précédentes.

#### **10.1.4 Cercles de confiance**

Dans la méthode des cercles de confiance, des groupes de personnes de confiance ou de personnes appartenant à des domaines de confiance se rassemblent et partagent leurs listes blanches. Le principe de cette méthode est qu'une personne fait confiance à un ami d'un ami de confiance. Le groupe forme une relation de confiance et peut décider d'appliquer un certain type de sanction si l'un de ses membres est pris en train d'envoyer des spams.

Une variante des cercles de confiance est la méthode de la liste noire répartie, dans laquelle un groupe de personnes partagent leurs listes noires. Cette méthode est très efficace pour filtrer les spams abusifs. De nombreux serveurs collectent les listes noires selon cette méthode et mettent la liste noire résultante à la disposition du grand public.

Ce type de méthode donne de bons résultats pour les petits groupes de fournisseurs pour lesquels le partage et l'application d'une telle politique sont faciles. Si la taille des cercles de confiance augmente, il est difficile de parvenir à un consensus sur le niveau approprié de sanction à appliquer en cas d'envoi de spams.

## **10.2 Masquage d'adresse**

Diverses applications multimédias IP ont besoin d'adresses pour l'utilisation de leurs services. Il est donc important de ne pas exposer son adresse au grand public. Mais, lors de l'utilisation de services web, les adresses doivent être présentées aux nouveaux clients pour que ceux-ci puissent prendre facilement contact avec le propriétaire. Les spammeurs exploitent cette faiblesse pour collecter des adresses cibles pour l'envoi de spams. Ils parcourent diverses pages web et collectent les adresses possédant la structure "@" et ".". Ils utilisent ensuite ces adresses pour envoyer des spams et communiquent ces adresses à d'autres spammeurs, car les spammeurs ont tendance à partager les adresses cibles.

Le masquage d'adresse est une méthode visant à occulter une adresse de sorte que les spammeurs ne puissent pas la collecter automatiquement. La méthode la plus simple consiste à remplacer "@" par AT et "." par DOT. L'adresse ressemble alors à du texte normal et n'est pas retenue par le système de filtrage automatique des adresses utilisé par les spammeurs.

Le masquage d'adresse n'est pas une méthode de lutte contre le spam, mais une méthode de prévention du spam. Cette méthode évite d'exposer les adresses au programme de collecte automatique des adresses utilisé par les spammeurs. Elle est donc utile pour éviter le spam dans les applications multimédias IP qui utilisent la même adresse pour les services web.

Le présent paragraphe décrit d'autres techniques pouvant être utilisées pour le masquage d'adresse.

### **10.2.1 JavaScript**

Dans l'environnement JavaScript, il est facile d'ajouter une adresse de type "[abc@xyz.com](mailto:abc@xyz.com)" en utilisant des fonctions Java. La page web affiche alors l'adresse sous la forme "[abc@xyz.com](mailto:abc@xyz.com)", mais lorsqu'on utilise la fonction document.write() en JavaScript, il est très facile d'occulter l'adresse de courrier électronique. Un exemple est présenté ci-dessous.

```
<SCRIPT TYPE="text/javascript">
  document.write('abc@' + 'xyz.com')
</SCRIPT>
```

Il est possible d'utiliser d'autres fonctions ou d'autres méthodes en JavaScript pour occulter l'adresse de courrier électronique. Mais il s'agit ici de décrire qu'il est possible d'occulter les adresses dans l'environnement JavaScript. Dans ce cas, il est difficile pour un spammeur de collecter automatiquement une adresse de courrier électronique, même si la page web affiche clairement une adresse de courrier électronique normale.

Cette méthode ne peut être utilisée que dans des environnements JavaScript. Mais si l'utilisateur souhaite mentionner son identificateur de messagerie instantanée ou son adresse de contact de VoIP sur une page web utilisant JavaScript, cette méthode permet de lui éviter de devenir une cible pour les spammeurs.

### **10.2.2 Code ASCII**

La méthode du code ASCII consiste à occulter sous forme de code ASCII ("&#number") des informations importantes, par exemple une adresse de courrier électronique ou un numéro de téléphone, cibles utilisées par les spammeurs. La page web n'est pas présentée sous forme de texte normal, mais sous forme d'image. Ainsi, lorsque la page web est téléchargée, on voit uniquement un code ASCII. Si le spammeur possède une fonction de conversion du code ASCII parmi ses outils de recherche dans les pages web, il pourra facilement décoder le code ASCII.

### **10.3 Preuve interactive pour les personnes**

Chaque utilisateur reçoit un puzzle ou un défi conçu de telle sorte que seules les personnes peuvent le reconnaître et pas les machines. Un puzzle ou un défi est une image ou le son d'un mot ou d'un nombre que seules les personnes peuvent comprendre et pas les machines. Il peut s'agir d'une image cachée derrière diverses couleurs ou d'un son caché derrière divers bruits, difficile à comprendre par une machine. Maintenant, il est plus difficile de créer des puzzles qui soient incompréhensibles par les machines, en raison des progrès réalisés dans les domaines du traitement automatique des images et des sons et de l'intelligence artificielle.

La méthode de la preuve interactive pour les personnes est en principe utilisée dans les applications web pendant une période d'abonnement à des services de réseau. Par conséquent, elle est bien adaptée à la lutte contre le spam sur le web. Elle peut aussi servir à filtrer les appels non sollicités avec une méthode d'autorisation utilisant des sons. Lorsqu'un appelant ne figurant ni sur la liste noire ni sur la liste blanche lance un appel vocal, le destinataire active automatiquement le système de réponse vocale interactive (IVR) pour demander à l'appelant de saisir un certain nombre sur le clavier du téléphone. Si l'appelant saisit correctement le nombre, le numéro de téléphone de l'appelant est ajouté automatiquement sur la liste blanche de l'utilisateur. La méthode de la preuve interactive peut être appliquée à un utilisateur d'un service de bavardage avant que celui-ci ne puisse participer à la conversation.

### **10.4 Filtrage du contenu**

Le filtrage du contenu de la ligne d'objet est la méthode la plus courante et la plus largement utilisée pour lutter contre le spam de courrier électronique. Cette méthode consiste à examiner la ligne d'objet à la recherche de mots suspects souvent utilisés dans les spams.

Les messages instantanés étant des messages de texte courts, ce mécanisme peut facilement être appliqué pour lutter contre le spam de messagerie instantanée. Le contenu de chaque message instantané peut être examiné par la même technologie que celle qui est utilisée pour examiner la ligne d'objet des courriers électroniques.

Toutefois, cette méthode n'est pas applicable pour le moment à la VoIP ou aux autres télécommunications multimédias IP qui incluent de l'audio et/ou de la vidéo. Les médias étant envoyés après l'établissement de l'appel, le préfiltrage du contenu ne présente aucun intérêt. Par ailleurs, même si un spam transmis sous forme de message vocal ou vidéo est stocké dans un serveur, la technologie actuelle de recherche de certains mots n'est pas suffisamment bonne pour être utilisée pour lutter contre le spam.

## **10.5 Authentification par échange de clé**

L'authentification permet d'identifier de façon sécurisée l'expéditeur de messages multimédias IP, ce qui permet de bloquer de nombreux spams découlant d'attaques par usurpation d'identité.

### **10.5.1 PKI et PGP**

Il est possible d'authentifier les expéditeurs afin de bloquer les demandes de connexion émanant de spammeurs se faisant passer pour quelqu'un d'autre, et notamment pour une personne figurant sur la liste blanche. L'infrastructure de clé publique (PKI) et le protocole Pretty Good Privacy (PGP) sont des méthodes d'authentification connues qui utilisent des mécanismes de clé publique. L'infrastructure PKI permet d'authentifier un expéditeur grâce à une clé publique certifiée par l'autorité de certification (CA). Le protocole PGP utilise un programme informatique qui assure une fonction de signature pour l'authentification. Dans les systèmes de courrier électronique, ces mécanismes sont utilisés pour chiffrer les messages et ajouter des signatures numériques. Il s'agit de mécanismes robustes pour éviter le spam.

Les mécanismes d'échange de clé sont utiles dans pratiquement tous les systèmes de télécommunication multimédia IP. Ils doivent être appliqués avec soin dans le cas des services de conférence IP, car le risque de vol de la clé de groupe d'une conférence est élevé.

Les méthodes PKI et PGP peuvent être utilisées dans pratiquement tous les types d'applications multimédias IP telles que la VoIP et la messagerie instantanée. Elles peuvent aussi être utilisées dans les applications web pour autoriser le postage de fichiers ou de messages uniquement par des personnes certifiées.

### **10.5.2 DKIM [b-IETF RFC 4871]**

La méthode du courrier identifié par clés de domaine (DKIM), élaborée par l'IETF (Internet Engineering Task Force), peut être utilisée pour l'authentification des courriers électroniques. Le serveur de courrier électronique joint une signature cryptographique au courrier pour valider le fait qu'il a réellement envoyé le courrier électronique en question. La méthode DKIM permet à une organisation de prendre la responsabilité d'un message devant être validé par le destinataire. Elle définit un cadre d'authentification de signature numérique au niveau des domaines pour les courriers électroniques fondé sur l'utilisation de la cryptographie à clé publique et de la technologie de serveur de clé. Un courrier électronique frauduleux peut causer un préjudice non seulement au destinataire mais aussi à la réputation d'une grande entreprise ou organisation. Le recours à la méthode DKIM permet de protéger l'entreprise ou l'organisation contre ces préjudices.

Le recours à la méthode DKIM permet d'éviter des communications frauduleuses par VoIP ou par messagerie instantanée. Le destinataire peut vérifier avec le serveur de l'expéditeur si le message ou l'appel reçu provient réellement de l'expéditeur déclaré. L'authentification peut se faire au début des communications, elle est donc sans incidence y compris pour les applications critiques en temps réel.

### **10.5.3 Authentification HTTP et connexion TLS**

L'utilisation de l'authentification HTTP Digest [b-IETF RFC 5090] associée à une connexion TLS (sécurité de la couche transport) avec le serveur est très efficace pour les applications multimédias IP avec une structure client-serveur. Le serveur d'un domaine valide ses utilisateurs par authentification HTTP Digest. L'authentification HTTP Digest est utilisée pour authentifier un

utilisateur d'application multimédia IP généralement au moyen d'un nom d'utilisateur et d'un mot de passe. Le client, à savoir l'utilisateur, maintient une connexion TLS persistante avec le serveur. Il vérifie l'identité du serveur en maintenant la connexion TLS avec le serveur. Celui-ci authentifie le client en utilisant un échange Digest sur la connexion TLS. Lorsqu'un utilisateur authentifié envoie un message à un autre domaine, le domaine d'expédition certifie l'utilisateur en insérant une signature pour valider le message. Les domaines d'expédition et de destination doivent s'authentifier mutuellement pour faire confiance aux utilisateurs de l'autre domaine.

Cette méthode peut être utilisée pour authentifier les utilisateurs qui communiquent par messagerie instantanée ou VoIP. L'authentification peut se faire au début des communications, elle est donc sans incidence y compris pour les applications critiques en temps réel.

## **10.6 Filtrage du spam dans le réseau**

Les mécanismes de filtrage du spam examinés ci-dessus ont été conçus pour fonctionner du côté serveur et du côté client des télécommunications. Mais il est également important de construire des réseaux sécurisés pour éviter le spam. Le présent paragraphe décrit brièvement certaines méthodes de filtrage du spam dans le réseau.

### **10.6.1 Rejet de paquets au niveau d'une entité de réseau**

Une certaine politique, par exemple une liste de contrôle d'accès (ACL), peut être utilisée dans un routeur ou une entité de réseau quelconque afin de rejeter les paquets soupçonnés d'être du spam provenant d'une adresse IP ou d'un préfixe IP d'origine particulier. Un spammeur peut être situé à l'intérieur ou à l'extérieur du réseau d'un ISP. Un ISP qui souhaite protéger son réseau contre le spam devra résoudre les deux problèmes avec des méthodes différentes.

Si le spammeur est situé à l'intérieur du réseau de l'ISP, l'ISP peut faire en sorte que l'entité de réseau dont relève ce spammeur coupe la connectivité IP dudit spammeur. Celui-ci se rendra compte que sa connectivité au réseau est perdue et sera contraint d'admettre ses mauvais agissements. Toutefois, il faut établir certains critères afin d'éviter les utilisations abusives. Une personne peut accuser à tort une personne innocente d'être un spammeur et lui couper sa connectivité au réseau. Une personne déloyale peut utiliser l'adresse IP d'une personne innocente pour envoyer des spams, entraînant aussi la coupure de la connectivité au réseau de cette personne innocente, l'envoi de spams pouvant durer un certain temps.

Supposons que le réseau de l'ISP A est raccordé au réseau de l'ISP B et qu'un spammeur utilise le réseau de l'ISP B. Si le spammeur est situé à l'extérieur du réseau de l'ISP A, l'ISP A doit vérifier si l'ISP B applique une politique de lutte contre le spam dans son réseau. Si ce n'est pas le cas, l'ISP A doit établir une politique antispam dans la passerelle de l'ISP B pour éviter l'inondation de spams dans le réseau de l'ISP A. Dans cette méthode, l'ISP A ne peut pas bloquer la connectivité au réseau du spammeur, mais il peut protéger son réseau contre le spam. Cette méthode permet de protéger et de sauvegarder les ressources de réseau. L'inconvénient de cette méthode est qu'elle peut bloquer la connexion au réseau de l'ISP A d'un utilisateur innocent de l'ISP B.

Un autre inconvénient de cette méthode est que le spammeur peut changer fréquemment d'adresse IP. L'ISP dont relève le spammeur doit donc contrôler et authentifier l'adresse IP utilisée par le spammeur pour que cette méthode fonctionne.

La méthode du rejet de paquets au niveau d'une entité de réseau peut être utilisée dans n'importe quelle application, car elle n'est pas liée aux applications multimédias IP.

### **10.6.2 Liste noire répartie**

Une liste noire répartie est une liste noire qui se trouve dans le réseau et qui est partagée par l'ensemble du réseau. Des listes noires réparties sont généralement mises en œuvre dans les serveurs DNS. Les utilisateurs peuvent ajouter sur la liste noire répartie une adresse à partir de laquelle du spam est envoyé. Une fois qu'une adresse IP apparaît sur une liste noire répartie, de nombreux sites

rejetent les messages provenant de cette adresse. L'applicabilité de cette méthode aux applications multimédias IP est équivalente à celle de la méthode de la liste noire.

### **10.6.3 Pare-feu antispam**

Les entreprises et les ISP utilisent des pare-feu antispam pour protéger leurs réseaux contre le spam. Un pare-feu antispam utilise de nombreuses méthodes mentionnées précédemment pour bloquer les spams avant qu'ils n'entrent dans le réseau. L'utilisateur d'un réseau protégé reçoit peu de spams. Cette méthode est une combinaison des méthodes de liste noire et de filtrage du contenu étant donné qu'elle tient à jour la liste noire et filtre le contenu à mesure que les paquets entrent dans le réseau d'entreprise.

Le pare-feu antispam est actuellement utilisé pour le courrier électronique et la messagerie instantanée. Cette méthode est inefficace pour les services de VoIP, car on ne peut rien saisir au début des appels de VoIP. Cette méthode peut être utilisée pour filtrer les spams sur le web, car un filtrage basé sur un examen du contenu est possible.

## **10.7 Timbre en ligne**

Dans la méthode du timbre en ligne, un expéditeur ne figurant pas sur la liste blanche du destinataire doit acheter un timbre en ligne pour envoyer un message. S'il envoie un message sans timbre en ligne, ce message sera rejeté par le serveur du fournisseur de service. Pour apparaître sur le terminal du destinataire, un message qui provient d'un expéditeur ne figurant pas sur la liste blanche doit avoir un timbre en ligne. Si le destinataire accepte le message, il renvoie le timbre en ligne à l'expéditeur et l'adresse de l'expéditeur est ajoutée automatiquement sur la liste blanche du destinataire. Si le destinataire décide que l'expéditeur est un spammeur, il peut garder l'argent du timbre en ligne. Plus le spammeur envoie de spams, plus ses dépenses augmentent.

Cette méthode peut être utilisée dans les services de courrier électronique, de VoIP et de messagerie instantanée. Comme l'expéditeur n'a à acheter un timbre en ligne qu'une seule fois, cette méthode n'est ni gênante ni onéreuse. Elle est donc efficace pour lutter contre le spam lorsqu'elle est utilisée avec un mécanisme approprié d'authentification d'identité de l'expéditeur.

## **10.8 Filtrage du spam basé sur une autorisation**

Un élément important pour le filtrage du spam est la mise en place d'un mécanisme dans lequel certaines entités du réseau sont chargées de "filtrer" les demandes de connexion entrantes en fonction des politiques de l'utilisateur et du réseau. Diverses entités, comme les utilisateurs et les administrateurs de système, peuvent créer et modifier les politiques d'autorisation. Une politique de réseau est nécessaire pour définir les flux de communication entre les domaines.

Les politiques d'autorisation peuvent être appliquées au niveau de l'hôte terminal et/ou par les éléments de réseau. L'entité qui établit les règles peut être un utilisateur final qui possède le dispositif, un fournisseur de service de VoIP, une personne ayant un lien avec l'utilisateur final (par exemple les parents d'un enfant utilisant un téléphone mobile). Le présent paragraphe porte sur divers mécanismes de filtrage du spam basés sur une autorisation.

### **10.8.1 Communications basées sur une permission**

Les communications basées sur une permission reposent sur une autorisation directe du message par le destinataire. Cette méthode est utilisée conjointement avec une liste blanche ou noire. Si un expéditeur ne figurant pas sur la liste noire ou blanche d'un utilisateur souhaite communiquer avec cet utilisateur, il lui envoie son identification et/ou un texte court pour s'identifier. L'expéditeur est d'abord rejeté. L'utilisateur est ensuite informé du fait que l'expéditeur souhaite communiquer avec lui. Il peut accepter ou refuser l'expéditeur après avoir examiné l'identification et/ou le texte court envoyé par l'expéditeur.

Ce type de méthode de filtrage est actuellement utilisé dans divers services de messagerie instantanée et s'avère très efficace pour la gestion de la liste blanche. Cette méthode est applicable aux appels, la permission étant obtenue au départ, mais elle ne convient pas pour le postage sur le web, qui est unidirectionnel. Elle est inadaptée pour les services faisant intervenir de multiples utilisateurs, car il serait inefficace de demander la permission de tous les participants aux services en cours.

L'inconvénient de cette méthode est que l'utilisateur peut être dérangé par des demandes de permission trop nombreuses. Il faudrait donc filtrer certaines des demandes de permission au moyen d'un autre système de filtrage.

### **10.8.2 Autorisation en fonction de la politique d'utilisateur**

Dans le cas de l'autorisation en fonction de la politique d'utilisateur, l'utilisateur multimédia IP définit une politique d'acceptation pour filtrer les demandes provenant d'expéditeurs inconnus. La politique est mise en œuvre au niveau du terminal de l'utilisateur ou du serveur d'application afin d'accepter ou de refuser automatiquement les demandes. La politique peut s'appliquer à l'adresse d'origine du spam, à l'identification et/ou au texte court envoyé par l'expéditeur comme dans le cas de la méthode des communications basées sur une permission. La politique peut aussi s'appliquer au contenu reçu (image, son ou texte) pour filtrer automatiquement les demandes de communication qui transgressent la politique. Les informations relatives aux demandes rejetées devraient être journalisées dans un répertoire, de sorte que l'utilisateur puisse consulter ces demandes et extraire celles qui n'auraient pas dû être rejetées. L'utilisateur peut modifier la politique pour répondre à ses besoins.

L'inconvénient de la méthode basée sur une permission est que l'utilisateur doit répondre à toutes les demandes de communication. En revanche, dans la méthode d'autorisation en fonction de la politique, la plupart des spams sont filtrés automatiquement de sorte que l'utilisateur n'est pas dérangé par le problème des demandes de permission trop nombreuses. L'établissement de la politique dépendra des caractéristiques des applications multimédias IP utilisées. La méthode de filtrage en fonction de la politique de l'utilisateur devrait être définie pour toutes les applications vulnérables aux spams.

Cette méthode s'avère très efficace pour la gestion des listes blanches. Étant donné qu'elle est basée sur l'utilisateur, elle peut être utilisée dans tout type de service bidirectionnel (par exemple VoIP et messagerie instantanée).

### **10.8.3 Autorisation en fonction de la politique de réseau**

Un opérateur de réseau devrait utiliser l'autorisation en fonction de la politique de réseau pour filtrer le spam et protéger le réseau. La politique de réseau peut être utilisée dans un seul réseau ou entre réseaux voisins. Cette méthode est équivalente à la méthode du rejet de paquets au niveau d'une entité de réseau.

Afin d'assurer un filtrage modulable du spam, l'opérateur de réseau peut déléguer une partie des droits d'administration à des utilisateurs finaux compétents et leur permettre de configurer la politique de réseau sur leurs liaisons avec le réseau du fournisseur. L'authentification nécessaire peut être mise en œuvre dans le routeur de service pour valider l'identité et les droits d'administration des utilisateurs. Seuls les utilisateurs valables sont autorisés à configurer les politiques de réseau conformément aux droits qui leur sont accordés.

## **10.9 Action en justice et réglementation**

Pour éviter le spam, il est important d'établir une réglementation et une législation visant à interdire le spam, même si leur efficacité fait débat. De nombreux pays ont établi des lois permettant aux victimes d'intenter une action en justice en cas de spam gênant. Le plus souvent, un publicitaire doit

insérer un ensemble spécial de contenus permettant aux destinataires de reconnaître les publicités, et il est sanctionné lorsque la règle est transgressée.

L'inconvénient de cette méthode est que l'on rencontre certaines difficultés lorsqu'il s'agit d'appliquer des lois antispam locales aux spams provenant de pays étrangers. Il faut établir un certain accord international entre de nombreux pays pour que cette méthode soit vraiment efficace. Des organismes internationaux comme l'UIT-T, l'OCDE, l'APEC, etc., essaient de définir une législation antispam efficace ainsi qu'une coopération et une mise en œuvre internationales.

Cette méthode n'est pas une méthode technique et elle n'est pas liée aux caractéristiques des applications multimédias IP.

## **11 Considérations relatives à la lutte contre le spam d'application multimédia IP**

Utiliser un réseau IP pour faire de la publicité n'est pas seulement économique, c'est aussi très efficace. Le spam est un problème qui provient de la mauvaise utilisation de la publicité. Il peut en résulter de graves problèmes de société (volume des publicités, fraude, attrait entraînant du harcèlement et préjudice causé aux utilisateurs du réseau).

Diverses méthodes de lutte contre le spam d'application multimédia IP ont été décrites dans la présente Recommandation. Les applications multimédias IP ayant des caractéristiques diverses, le spam les concernant peut aussi prendre des formes diverses. Le recours à seulement une ou deux méthodes ne permettra pas de lutter contre tous les types de spam multimédia IP. Pour vraiment résoudre le problème du spam ou du moins l'atténuer, il faut étudier en détails les divers types de spam concernant les diverses entités d'application multimédia. Par conséquent, les méthodes de lutte contre le spam doivent être analysées en fonction des caractéristiques des applications multimédias IP. Le présent paragraphe tente de décrire certains éléments à prendre en considération dans la lutte contre le spam d'application multimédia IP.

Pour lutter efficacement contre le spam d'application multimédia IP, il faut tenir compte d'approches différentes pour chacun des groupes de participants aux services, à savoir: utilisateurs de service (et/ou abonnés à un service), fournisseurs de service, opérateurs de réseau, organismes publics et publicitaires. Ainsi, le présent paragraphe décrit certains éléments à prendre en considération dans la lutte contre le spam d'application multimédia IP concernant chaque groupe.

### **11.1 Utilisateur de service (abonné à un service)**

Les utilisateurs de service et/ou les abonnés à un service sont les véritables victimes du spam et devraient être conscients de l'importance du blocage des spams afin de protéger leurs droits. On indique ci-après certains éléments qu'un utilisateur de service devrait prendre en considération dans la lutte contre le spam, même si l'application de ces suggestions peut varier en fonction du média:

- Les utilisateurs devraient se procurer des moteurs de filtrage du spam et les tenir à jour afin de bloquer les spams. Etant donné que de nouveaux spams peuvent toujours apparaître, les moteurs de filtrage doivent être mis à jour afin de limiter les nouveaux spams.
- Les utilisateurs devraient s'abonner à divers systèmes de filtrage du spam, par exemple de type liste noire ou liste blanche, et mettre à jour en permanence les listes associées à ces systèmes.
- Lorsque les utilisateurs rencontrent un spam, ils devraient l'éliminer immédiatement et informer le grand public de ce problème afin d'éviter qu'il y ait d'autres victimes.
- Les utilisateurs devraient participer à des formations à la prévention du spam afin de connaître les nouveaux spams et les nouvelles techniques de lutte antispam. De nouveaux types de spams peuvent apparaître dans les services classiques comme dans les nouveaux services. Cela étant, il n'est pas nécessaire d'utiliser toutes les techniques de lutte antispam, mais il convient d'essayer de trouver une solution adéquate afin de limiter les spams.

- Les utilisateurs devraient veiller à protéger leurs informations personnelles des spammeurs. Ils ne devraient pas utiliser des identifications ou des numéros faciles à retenir ou faciles à deviner.
- Les utilisateurs devraient utiliser des techniques de prévention pour bloquer les demandes de communication provenant de spammeurs et configurer leur système de manière à rendre les communications difficiles pour les spammeurs.

## 11.2 Fournisseur de service

Il peut être très avantageux pour les fournisseurs de service d'offrir un service de qualité. Les spams peuvent causer des dommages importants au service, étant donné que les spammeurs utilisent abusivement le service. Les fournisseurs de service devraient être conscients du problème du spam afin de protéger leur réseau et d'offrir des services meilleurs. On indique ci-après certains éléments que les fournisseurs de service peuvent prendre en considération dans la lutte contre le spam:

- Avant de lancer un nouveau service multimédia IP, un fournisseur de service peut réaliser une analyse des risques que le nouveau service soit la cible de spams potentiels. Les services multimédias IP ne sont pas tous des cibles pour les spammeurs. La réalisation de cette analyse et l'élaboration de solutions rendant difficile la propagation de spams augmenteront les chances de succès des nouveaux services. Si un service sensible au spam est mis en place sans ce processus, il sera difficile de limiter le spam et les utilisateurs finiront par se désintéresser du nouveau service après avoir été victimes de spams.
- Les fournisseurs de service peuvent vérifier toutes les entités (utilisateurs, réseaux, éléments de service, etc.) qui constituent le service ou l'application multimédia IP et analyser diverses méthodes antispam dans chaque entité afin de trouver des solutions simples et efficaces pour combattre les spams. Il est possible d'utiliser des techniques de lutte contre le spam uniquement dans le cadre du service multimédia IP, mais de meilleures solutions peuvent être trouvées lorsqu'on considère l'ensemble des entités de réseau.
- Les fournisseurs de service peuvent rechercher en permanence l'apparition de nouveaux spams dans les applications classiques. De nouveaux types de spam peuvent apparaître y compris dans les services les plus anciens. Les fournisseurs de service souhaiteront peut-être repérer ce type de phénomène et essayer de trouver des solutions pour les nouveaux types de spam, y compris dans les anciens services.
- Les fournisseurs de service peuvent utiliser divers filtres, par exemple de type liste noire ou liste blanche, pour contrôler l'accès des utilisateurs au service. Le mieux est d'éviter que les spammeurs utilisent le service, car les spammeurs ne feront rien d'autre que d'utiliser abusivement le service.
- Si le service nécessite un abonnement, le fournisseur de service peut rendre le processus d'abonnement suffisamment difficile pour dissuader les spammeurs de s'abonner au service. Un grand nombre de spammeurs utilisent des méthodes automatiques ou recrutent des employés bon marché pour avoir de nombreux abonnements, ce qui est très efficace pour l'envoi de spams. Le processus d'abonnement peut contenir des méthodes d'authentification forte pour vérifier l'abonné et peut être doté d'un mécanisme permettant d'éviter qu'un même utilisateur puisse avoir des abonnements multiples et que les spammeurs puissent s'abonner au service.
- Si une liste d'utilisateurs est associée au service, le fournisseur de service peut disposer d'une méthode permettant d'évaluer la crédibilité d'un utilisateur donné pour éviter que cet utilisateur utilise abusivement le service ou commette des abus vis-à-vis des autres utilisateurs du service. Le fournisseur de service devrait mettre en œuvre une technique de protection pour éviter que des utilisateurs internes ou externes exposent des informations personnelles relatives aux abonnés.

- Si un répertoire est associé au service, le fournisseur de service souhaitera peut-être surveiller le contenu du site web afin de supprimer le spam. On peut réaliser une analyse du contenu, y compris des données vidéo et audio, pour rechercher les contenus inappropriés.
- Le fournisseur de service peut choisir d'offrir aux utilisateurs du service une méthode leur permettant de limiter le spam. Il peut s'agir d'un moteur de filtrage, d'une liste de filtrage, d'outils de configuration de la politique, de manuels de lutte contre le spam ou de toute autre chose qui peut servir aux utilisateurs pour combattre le spam.

### 11.3 Opérateur de réseau

Le spam peut entraîner un gaspillage des ressources de réseau, en particulier s'il a un contenu multimédia. Les opérateurs de réseau devraient tenter de bloquer les spams afin de protéger leur réseau et d'assurer des services de réseau efficaces. On indique ci-après certains éléments que les opérateurs de réseau devraient prendre en considération dans la lutte contre le spam:

- Les opérateurs de réseau peuvent surveiller le trafic dans le réseau et rechercher le trafic anormal qui peut être considéré comme du spam. Ils devraient pouvoir analyser le trafic anormal et prendre une mesure appropriée. Il n'est pas facile de saisir les spams en analysant le trafic dans le réseau. Néanmoins, divers spams ou programmes malveillants ont tendance à se présenter sous forme de trafic anormal.
- Les opérateurs de réseau peuvent limiter les spams ou effectuer toute autre tâche permettant de stopper les spams.
- Les opérateurs de réseau peuvent coopérer avec le fournisseur de service en partageant des informations liées aux spams. Ils peuvent réellement stopper les spams, rendant ainsi inutile l'envoi de spams.
- Les opérateurs de réseau peuvent utiliser divers pare-feu antispam pour protéger le réseau.
- Les réseaux peuvent être configurés uniquement avec des réseaux de confiance, de sorte que les utilisateurs qui sont authentifiés et autorisés par un réseau de confiance puissent communiquer. Si les réseaux possèdent ce type de relations de confiance, il est possible pour chaque réseau de contrôler le trafic et les utilisateurs. Au bout du compte, la totalité du réseau peut être protégée contre les spams et autre trafic malveillant lorsque tous les sous-réseaux font confiance au trafic provenant des sous-réseaux homologues.

### 11.4 Organisme public

Un organisme public peut être un organisme gouvernemental ou un organisme privé constitué de groupes d'intérêt qui œuvrent dans la lutte contre le spam. L'organisme privé peut être une association à but lucratif ou à but non lucratif qui possède une solution efficace pour limiter le spam. On indique ci-après certains éléments que les organismes publics souhaiteront peut-être prendre en considération dans la lutte contre le spam:

- Les organismes publics peuvent avoir un système qui permette aux victimes de spams de soumettre un rapport sur le préjudice subi. Ils peuvent mettre en garde ou sanctionner les spammeurs. Il peut s'agir d'organismes gouvernementaux ou d'organismes privés puissants capables de mettre en garde efficacement les spammeurs.
- Les organismes publics pourront choisir d'avoir un programme de formation ou de donner des recommandations aux utilisateurs de service multimédia IP, aux fournisseurs de service multimédia IP et aux opérateurs de réseau IP concernant la lutte contre le spam. La lutte contre le spam nécessite une expérience approfondie, à laquelle les nouveaux fournisseurs de service multimédia IP et opérateurs de réseau IP ne sont peut-être pas préparés.
- Les organismes publics peuvent disposer de listes noires ou de filtres qui peuvent être utilisés en partage par le grand public, lequel peut participer à la construction des listes noires ou des filtres.

- Il serait utile pour les agences de publicité de prévoir un système d'approbation des publicités non falsifiable et authentifié qu'elles peuvent utiliser sans être prises par erreur pour des spammeurs.

### **11.5 Autres considérations**

D'autres considérations, qui ne sont pas liées aux considérations mentionnées ci-dessus, sont les suivantes:

- Le problème du spam ne disparaîtra probablement pas, quelles que soient les diverses activités de recherche menées pour lutter contre ce fléau. De nouveaux spams apparaîtront toujours et de nouvelles études devront être réalisées pour les combattre. Mais si des travaux de recherche concernant les méthodes de lutte contre le spam sont réalisés en amont, on peut améliorer les environnements des applications et améliorer ainsi les services d'application offerts.
- Diverses méthodes de lutte contre le spam doivent être combinées. Actuellement, il n'existe pas de supersolution au problème du spam. Diverses méthodes fondées sur différentes techniques doivent être combinées pour combattre les divers types de spam que l'on peut rencontrer dans différents endroits.
- La solution optimale consiste peut-être à rendre difficile et onéreux l'envoi de spams. Les spammeurs cherchent avant tout à employer une méthode publicitaire simple et bon marché. Ils finiront par arrêter d'envoyer des spams si cette activité devient difficile et onéreuse ou si les sanctions appliquées sont trop fortes.

## Bibliographie

- [b-UIT-T Q.814] Recommandation UIT-T Q.814 (2000), *Spécification d'un agent interactif d'échange informatisé de données.*
- [b-UIT-T T.124] Recommandation UIT-T T.124 (1998), *Commande générique de conférence.*
- [b-UIT-T T.180] Recommandation UIT-T T.180 (1998), *Mécanisme d'accès homogène aux services de communication.*
- [b-UIT-T X.509] Recommandation UIT-T X.509 (2005) | ISO/CEI 9594-8:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*
- [b-UIT-T X.741] Recommandation UIT-T X.741 (1995) | ISO/CEI 10164-9:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: objets et attributs de contrôle d'accès.*
- [b-IETF RFC 1991] IETF RFC 1991 (1996), *PGP Message Exchange Formats.*  
<<http://www.ietf.org/rfc/rfc1991.txt?number=1991>>.
- [b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging.* <<http://www.ietf.org/rfc/rfc3428.txt?number=3428>>.
- [b-IETF RFC 4871] IETF RFC 4871 (2007), *DomainKeys Identified Mail (DKIM) Signatures.*  
<<http://www.ietf.org/rfc/rfc4871.txt?number=4871>>.
- [b-IETF RFC 4880] IETF RFC 4880 (2007), *OpenPGP Message Format.*  
<<http://www.ietf.org/rfc/rfc4880.txt?number=4880>>.
- [b-IETF RFC 4981] IETF RFC 4981 (2007), *Survey of Research towards Robust Peer-to-Peer Networks: Search Methods.*  
<<http://www.ietf.org/rfc/rfc4981.txt?number=4981>>.
- [b-IETF RFC 5039] IETF RFC 5039 (2008), *The Session Initiation Protocol (SIP) and Spam.*  
<<http://www.ietf.org/rfc/rfc5039.txt?number=5039>>.
- [b-IETF RFC 5090] IETF RFC 5090 (2008), *RADIUS Extension for Digest Authentication.*  
<<http://www.ietf.org/rfc/rfc5090.txt?number=5090>>.



## SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
<b>Série X</b>	<b>Réseaux de données, communication entre systèmes ouverts et sécurité</b>
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication