Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1231

(04/2008)

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

Sécurité du cyberespace – Lutte contre le pollupostage

Stratégies techniques de lutte contre le spam

Recommandation UIT-T X.1231

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	X.1000–
APPLICATIONS ET SERVICES SÉCURISÉS	X.1100–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	**X.1230–X.1249**
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	X.1300–X.1399

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

Recommandation UIT-T X.1231

Stratégies techniques de lutte contre le spam

Résumé

La Recommandation UIT-T X.1231 porte sur les stratégies techniques de lutte contre le spam et décrit également les caractéristiques générales du spam et les principaux objectifs de la lutte contre le spam. Elle contient en outre, faute d'une solution unique pour résoudre le problème du spam, une liste de vérifications à faire pour évaluer les outils prometteurs de lutte contre le spam.

Source

La Recommandation UIT-T X.1231 a été approuvée le 18 avril 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

Lutte contre le spam, spam, stratégies techniques.

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 [avait/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/.

TABLE DES MATIÈRES

		Page
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	1
4	Abréviations et acronymes	2
5	Conventions	3
6	Considérations générales	3
7	Objectifs génériques	5
8	Stratégies techniques	6
	8.1 Stratégies relatives aux équipements	7
	8.2 Stratégies relatives au réseau	8
	8.3 Stratégies relatives aux services	9
	8.4 Stratégies relatives au filtrage	10
	8.5 Stratégies relatives au retour de l'information	12
9	Evaluation des systèmes	12
Bibliographie		14

Introduction

Parallèlement au développement du secteur de l'information, la généralisation du spam constitue aujourd'hui un problème endémique qui engendre des manques à gagner pour les opérateurs de télécommunication, les fournisseurs de services et les utilisateurs commerciaux et qui a des effets préjudiciables sur les utilisateurs en général. De simple nuisance qu'il était au départ, le spam est devenu un véritable fléau mondial.

Il est donc nécessaire de trouver des moyens efficaces et rationnels pour lutter contre le spam. Cette lutte peut être menée sur différents plans: au niveau de la législation, de la formation, de la coopération internationale, etc. La présente Recommandation est essentiellement axée sur les moyens techniques.

Recommandation UIT-T X.1231

Stratégies techniques de lutte contre le spam

1 Domaine d'application

La présente Recommandation porte sur les stratégies techniques de lutte contre le spam et décrit également les caractéristiques générales du spam et les principaux objectifs de la lutte contre le spam. Elle contient en outre, faute d'une solution unique pour résoudre le problème du spam, une liste de vérifications à faire pour évaluer les outils prometteurs de lutte contre le spam.

Portant sur les stratégies techniques de manière générale, la présente Recommandation n'entre pas dans le détail des stratégies techniques pour tel ou tel type de spam. En outre, elle indique un modèle hiérarchique de catégories générales pouvant servir à mettre en place une infrastructure efficace et rationnelle de lutte contre le spam. Ce modèle comprend les parties suivantes:

- stratégies relatives aux équipements;
- stratégies relatives au réseau;
- stratégies relatives aux services;
- stratégies relatives au filtrage;
- stratégies relatives au retour de l'information.

Dans la pratique, la présente Recommandation définit les stratégies techniques de lutte contre les divers types de spam qu'une administration juge inappropriés, conformément à sa législation et à ses politiques nationales.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 authentification [b-UIT-T X.811]: attestation de l'identité revendiquée par une entité.

3.1.2 poste téléphonique IP [b-UIT-T Q-Sup.49]: terminal (par exemple terminal vocal spécialisé ou ordinateur personnel multifonctions) directement connecté (par exemple par une interface Ethernet ou une ligne xDSL) à un réseau IP.

3.1.3 entité de messages courts (SME, *short message entity*) [b-UIT-T Q.1742.3]: entité qui compose et décompose les messages courts. Une entité SME peut être ou non située dans un registre HLR, un centre MC, un registre VLR, une station MS ou un centre MSC et être impossible à distinguer de celui-ci.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 messagerie instantanée (IM, *instant messaging*): transfert de messages entre utilisateurs presqu'en temps réel. Ces messages sont généralement, mais pas nécessairement, courts. La messagerie instantanée est souvent utilisée en mode conversationnel car le transfert de messages dans les deux sens est suffisamment rapide pour que les participants puissent maintenir une conversation interactive.

3.2.2 spam multimédia IP: messages ou appels non sollicités sur des applications multimédias IP en temps réel. Différent du spam traditionnel par courrier électronique, le spam multimédia IP désigne le spam sur les nouvelles méthodes de communication sur IP, telles que la messagerie instantanée, le service de présence, la voix sur IP (VoIP), etc. Le spam sur téléphonie Internet (SPIT), le spam vocal ou spam VoIP (VAM) et le spam sur messagerie instantanée (SPIM) désignent aujourd'hui différents types de spam multimédia IP.

3.2.3 modalité: ce terme s'applique au codage des informations, dont certaines sont perceptibles par les êtres humains. Comme exemples d'informations de modalité, citons les données textuelles, graphiques, audio, vidéo ou tactiles utilisées dans une interface homme-ordinateur. Les informations multimodales peuvent être reçues en provenance ou être émises à destination de dispositifs multimodaux tels qu'un microphone pour un dispositif de saisie de données vocales/sonores, un stylet pour un dispositif de saisie de données tactiles, un clavier pour un dispositif de données textuelles, une souris pour un dispositif de saisie de données vidéo, un haut-parleur pour la restitution de signaux de synthèse vocale, un écran pour l'affichage de données graphiques/textuelles, un dispositif vibreur pour alarme tactile ou un système d'écriture braille pour malvoyants.

3.2.4 message multimodal: type de message multimédia contenant différentes informations codées permettant des interactions selon diverses modalités.

3.2.5 service de messagerie multimédia (MMS, *multimedia messaging service*): type de service de messagerie postérieur au service de messages courts qui permet de transférer divers messages multimédias contenant des données textuelles, graphiques, audio, vidéo, etc., via un réseau mobile, sans fil ou fixe.

3.2.6 service de messages courts (SMS, *short message service*): type de service de messagerie permettant aux téléphones mobiles, téléphones fixes et autres entités de messages courts de transférer et recevoir des messages texte via un dispositif appelé centre de service mettant en œuvre des fonctions telles que la sauvegarde et la remise.

3.2.7 spammeur: entité ou personne qui crée et envoie des spams.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

DDoS déni de service réparti (*distributed denial of service*)

DoS déni de service (*denial of service*)

E-mail courrier électronique (*electronic mail*)

HLR registre de localisation de rattachement (*home location register*)

IM messagerie instantanée (*instant messaging*)

IP protocole Internet (*Internet protocol*)

MC centre de messages (*message centre*)

MMS service de messagerie multimédia (*multimedia messaging service*)

MS station mobile (*mobile station*)

MSC centre de commutation mobile (*mobile switching centre*)

RTPC réseau téléphonique public commuté

SME entité de messages courts (*short message service*)

SMS service de messages courts (*short message service*)

SMTP protocole simple de transfert de courrier (*simple mail transfer protocol*)

SPIM spam sur messagerie instantanée (*spam over instant messaging*)

SPIT spam sur téléphonie Internet (*spam over Internet telephony*)

VAM spam vocal ou spam VoIP (*voice spam or VoIP spam*)

VLR registre des positions des visiteurs (*visitor location register*)

VoIP voix sur IP (*voice over IP*)

5 Conventions

Aucune.

6 Considérations générales

Le spam désigne la diffusion, par des expéditeurs à des destinataires, à partir de terminaux tels que ordinateurs, téléphones mobiles, téléphones fixes, etc., d'informations électroniques généralement non sollicitées, indésirables et préjudiciables pour les destinataires. Ces informations peuvent être acheminées par courrier électronique, service de messagerie mobile, services multimédias IP et sous d'autres formes électroniques. En fait, la définition du "spam" varie selon les perceptions des pays, des organisations ou des particuliers. Sa définition évolue et s'étend à de nouveaux domaines avec le développement des technologies de l'information et de la communication qui offrent de nouvelles possibilités de diffusion du spam. En règle générale, le spam a pour caractéristiques communes d'être:

Electronique: le spam désigne des informations électroniques qui sont généralement transmises dans un réseau de télécommunication ouvert, en particulier l'Internet, ce qui le différencie radicalement des méthodes de diffusion massive traditionnelles par courriers postaux, prospectus publicitaires ou marketing direct. Le spam est bon marché, commode et facile à dissimuler.

Non sollicité: le spam contient généralement des annonces publicitaires, des informations frauduleuses, des virus, etc.

En outre, le spam présente généralement l'ensemble des caractéristiques suivantes ou certaines d'entre elles:

Massif et répétitif: les messages et courriers électroniques non sollicités (spam) sont généralement envoyés en masse de manière systématique, alors que les communications non sollicitées en temps réel sont généralement lancées de manière répétitive. Cela étant, les spammeurs ne connaissent généralement que l'adresse de communication du destinataire (adresse de courrier électronique ou numéro de téléphone du destinataire, par exemple).

Utilisation d'adresses sans le consentement du propriétaire: les spammeurs utilisent souvent, pour envoyer des spams, des adresses de communication recueillies sans le consentement explicite du propriétaire. Dans la pratique, certains programmes logiciels recueillent des adresses de communication sur le web ou créent des adresses de communication automatiquement.

Origine des messages cachée ou fausse: l'envoi d'un spam est souvent effectué en dissimulant l'expéditeur sous un faux en-tête de message ou simplement en cachant le nom de l'expéditeur. Les spammeurs utilisent généralement des serveurs non autorisés de tiers qui ne valident pas les informations relatives à l'expéditeur.

Difficulté des tentatives de blocage: les spams sont très difficiles à détecter du fait qu'ils sont envoyés en raison du grand nombre de messages. Les tentatives de blocage des spams peuvent se révéler difficiles et, parfois, donneront lieu à de faux positifs ou de faux négatifs.

Les stratégies utilisées devraient être technologiquement neutres, tout en permettant d'évaluer un certain nombre de facteurs: les moyens de communication qui font l'objet d'une utilisation abusive ou qui causent des problèmes dans la circonscription considérée, les moyens de communication qui sont très susceptibles de faire l'objet d'une utilisation abusive dans l'avenir et les moyens de communication qui sont peu susceptibles de faire l'objet d'une utilisation abusive. Les options courantes sont les suivantes:

Courrier électronique

A l'heure actuelle, le spam par courrier électronique constitue la menace la plus importante parmi les divers types de spam en raison des vulnérabilités du protocole de courrier électronique et des failles de sécurité de l'infrastructure de base, c'est-à-dire de l'Internet, par lequel les courriers électroniques sont transmis. Le protocole simple de transfert de courrier (SMTP*)* est le protocole le plus répandu pour la retransmission des messages électroniques. Le protocole SMTP définit une enveloppe et un en-tête pour un message électronique. L'enveloppe contient l'adresse du destinataire que celui-ci ne peut pas voir. Elle est utilisée comme adresse de destination pour le transfert des messages de l'expéditeur jusqu'au destinataire. Normalement, pendant la transmission, l'adresse de destination figurant dans l'enveloppe est reproduite dans l'en-tête du message électronique qui est visible par le destinataire. Les spammeurs exploitent deux types de vulnérabilité dans le processus d'authentification SMTP:

- la dispense d'authentification, qui permet aux utilisateurs de cacher ou de falsifier leurs adresses;
- la possibilité de falsifier la plupart des informations figurant dans l'enveloppe ou l'en-tête des messages électroniques.

De plus, le coût d'envoi d'un spam par courrier électronique est très faible alors que ses effets négatifs sont toujours très importants.

Service de messagerie mobile

Les communications mobiles ont pour avantages remarquables d'être pratiques, efficaces, économiques et faciles à utiliser. Toutefois, aujourd'hui, les utilisateurs sont confrontés au spam par messagerie mobile tout en jouissant des avantages des communications mobiles. On désigne généralement sous le terme de "spam par messagerie mobile" les messages non sollicités envoyés par SMS ou MMS. Actuellement, les principaux types de spam par messages courts sont les suivants:

- messages dolosifs incitant les utilisateurs à s'abonner à un service;
- messages publicitaires;
- messages trompeurs illicites;
- messages à caractère pornographique.

Ces types de messages, qui sont généralement trompeurs ou frauduleux, sont également désignés sous le nom de scams (tentative d'escroquerie par courrier électronique).

Il importe de noter qu'il est aujourd'hui courant, avec l'apparition des services de courrier électronique mobile, de recevoir des messages électroniques sur des dispositifs mobiles. En effet, ces services sont plus faciles à utiliser par les spammeurs.

Services multimédias IP

Avec le développement des services multimédias IP, le concept de spam commence à s'appliquer de manière générale aux services multimédias IP de messagerie instantanée, de téléphonie Internet, de présence, de blog, de groupe de nouvelles usenet, de messagerie de jeu en ligne, etc. Dans certains cas, on emploie des terminologies différentes selon le type de moyen utilisé pour acheminer le spam, par exemple SPIM (spam sur messagerie instantanée), SPIT (spam sur

téléphonie Internet), etc. En outre, les interactions multimodales, en tant que nouveaux types de multimédia, sont également affectées par le spam, un spam multimédia unique pouvant prendre diverses formes sur les interfaces utilisateur. Ainsi, un spam de type message de réseau peut déclencher, de manière non sollicitée, la lecture d'un clip audio, la visualisation d'un clip vidéo et l'affichage d'un message texte sur l'écran, chacun d'entre eux avec un contenu identique ou différent. Toutefois, les multimodalités augmentent le risque d'exposition au spam multimédia et il faut donc s'attendre à un accroissement du problème du spam multimodal lorsque les interactions multimodales se généraliseront.

SPIM: la messagerie instantanée compte parmi les méthodes de communication pratiques, en temps réel et économiques qui se développent rapidement sur l'Internet. Elle est essentiellement utilisée pour les communications privées. Cela étant, les applications de messagerie instantanée sont de plus en plus utilisées dans les entreprises. Malheureusement, de plus en plus d'informations illicites, telles que virus, codes malveillants, etc. (communément désignées par l'abréviation SPIM), sont diffusées par le biais de la messagerie instantanée. Bien qu'il ne représente qu'un faible pourcentage de tous les spam, le spam sur messagerie Internet (SPIM) augmente rapidement.

SPIT: parmi les problèmes de spam qui ont été recensés jusqu'à présent, outre ceux qui sont généralement associés aux réseaux IP, citons d'autres menaces plus élaborées telles que la fausse déclaration, l'écoute clandestine, les attaques par déni de service en VoIP, l'injection de paquets et les messages non sollicités (spam sur VoIP, ou SPIT). Cette dernière menace tient principalement à la possibilité qu'offre la VoIP d'envoyer des messages vocaux à un coût très faible, ce qui pourrait déboucher sur une situation comparable à celle que l'on a déjà connue avec le spam par courrier électronique: un grand nombre de messages de boîte vocale non sollicités peuvent être envoyés dans le monde entier en l'espace de quelques secondes.

Evolution du spam

Le spam ne se limite pas aux options susmentionnées. Avec l'apparition de plus en plus de technologies et applications de l'information et de la communication, le spam évoluera de façon ubiquitaire. En outre, n'importe quelle technologie ou application de communication peut servir de moyen de diffusion du spam si les solutions proposées de lutte contre le spam sont inefficaces.

7 Objectifs génériques

Le présent paragraphe a pour objet de définir les finalités de la lutte contre le spam. Il s'agit, non pas de définir des modalités de mise en œuvre pratique, mais de s'attacher au résultat à obtenir.

Les objectifs de la lutte contre le spam sont les suivants:

- Validation de la question de savoir si les entités possèdent des privilèges pour envoyer des messages ou lancer des communications après authentification et/ou avec autorisation.
- Protection contre la dissimulation et le masquage de l'adresse et/ou des autres informations importantes des messages ou communications envoyés par des entités légitimes.
- Protection des données personnelles pendant la transmission des informations.
- Responsabilité de la part de toutes les entités au sujet de leurs propres comportements en matière de transmission ou retransmission de l'information.
- Protection des réseaux de télécommunication contre toute tentative d'accès ou d'exploitation non autorisée afin d'en assurer l'accessibilité de manière efficace et rationnelle.
- Fourniture des informations nécessaires sur l'expéditeur à des fins de traçabilité future.
- Protection des équipements de service contre les virus et tout accès non autorisé afin de garantir la disponibilité.
- Filtrage des spams et, si nécessaire, stockage des spams dans certains équipements à des fins de traçabilité et d'analyse forensique.

- Mise en place d'une plate-forme de collecte des réactions qui non seulement encourage la communication précise et efficace d'informations mais qui serve également de support pour la coopération internationale, l'élaboration des lois, etc.
- Application de protocoles internationaux bien établis pour l'échange et la diffusion d'informations pertinentes de lutte contre le spam.

Qui plus est, la réalisation des objectifs susmentionnés devrait être adaptée à l'environnement considéré.

8 Stratégies techniques

En matière de lutte contre le spam, une approche diversifiée s'impose, qui porte sur les aspects suivants: technologie développée par le secteur privé, autodiscipline des entreprises, coopération internationale, législation, collecte des réactions et formation. Parmi ces aspects, la technologie est essentielle pour garantir la mise en œuvre des autres aspects. La présente Recommandation porte essentiellement sur les stratégies techniques générales de lutte contre le spam.

Afin de faciliter l'analyse, il est préférable de commencer par classer les services. Selon la méthode de transmission utilisée, les services peuvent être classés dans la catégorie "enregistrement et retransmission" ou dans la catégorie "communication en temps réel". La catégorie "enregistrement et retransmission" comprend les services de courrier électronique, les services de messagerie mobile, les services de messagerie multimédia, etc. La catégorie "communication en temps réel" comprend la téléphonie IP, la télécopie IP, la messagerie instantanée, etc. Les méthodes de lutte contre le spam diffèrent d'un service à l'autre. Il faut donc procéder à une analyse détaillée pour tel ou tel service sur la base des stratégies techniques générales.

Pour lutter efficacement contre le spam, il est recommandé de mettre en œuvre un modèle hiérarchique en plusieurs parties, étant entendu que, plus les parties mises en place seront nombreuses, plus l'efficacité sera grande. La Figure 1 représente le modèle hiérarchique de lutte contre le spam, dont une description est donnée ci-après:

<table>
<tr><td>Stratégies relatives au filtrage</td><td>Stratégies relatives au retour de l'information</td></tr>
<tr><td colspan="2">Stratégies relatives aux services</td></tr>
<tr><td>Stratégies relatives aux équipements</td><td>Stratégies relatives au réseau</td></tr>
</table>

Figure 1 – Modèle hiérarchique de lutte contre le spam

Les cinq parties de ce modèle hiérarchique sont subdivisées en trois niveaux: la couche infrastructure, la couche service et la couche application. Les stratégies relatives aux équipements et les stratégies relatives au réseau, qui relèvent de la couche infrastructure, constituent les éléments de base du modèle hiérarchique. Ces éléments constituent une assise sûre et fiable pour les stratégies techniques dans les couches supérieures. Les stratégies relatives aux équipements et les stratégies relatives au réseau sont interdépendantes. Des réseaux sécurisés exigent des équipements sécurisés, cependant que des équipements sécurisés exigent des réseaux raisonnables. Les stratégies relatives aux services, qui relèvent de la couche service, constituent la plus importante des cinq parties, étant donné que la couche service est directement responsable de la fourniture des services. Enfin, les stratégies relatives au filtrage et les stratégies relatives au retour de l'information, qui relèvent de la couche application, sont les plus proches des utilisateurs aux fins de la lutte contre le spam; toutefois, elles interagissent les unes avec les autres. La Figure 2 représente la relation entre les différentes parties:

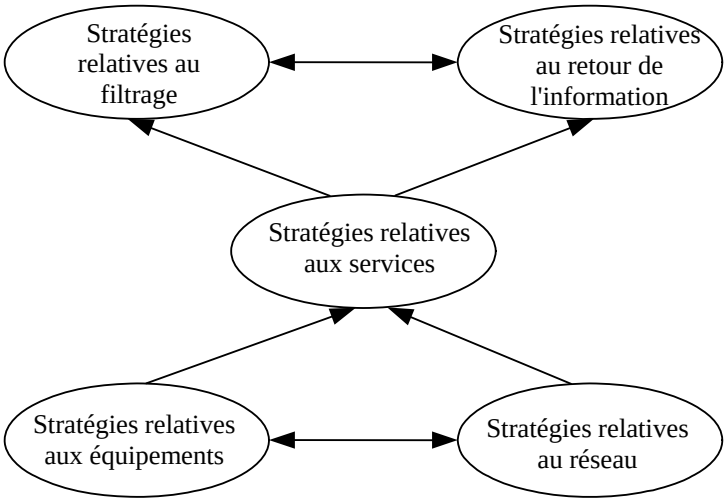

Figure 2 – Relation entre les différentes parties

En outre, il est recommandé d'utiliser des protocoles internationaux bien établis pour mettre en œuvre ces stratégies techniques. Mais si toutes les stratégies techniques sont mises en œuvre, le coût de l'opération peut se révéler trop élevé par rapport à la valeur des services protégés. Il est donc très important d'adapter les stratégies techniques aux besoins de l'utilisateur en fonction des scénarios d'application. De plus, les méthodes de lutte contre le spam devraient être fournies d'une manière qui permette une adaptation aux besoins de l'utilisateur. En raison du grand nombre de combinaisons de stratégies techniques possibles, il est souhaitable de disposer de profils qui couvrent une large gamme de services. La normalisation par l'intermédiaire d'entreprises privées et d'organismes de recherche facilitera la réutilisation de solutions et de produits, ce qui permettra de déployer des solutions techniques de lutte contre le spam plus rapidement et pour un prix inférieur.

8.1 Stratégies relatives aux équipements

Les équipements constituent le socle de l'infrastructure de lutte contre le spam. La protection des équipements est donc essentielle dans la lutte contre le spam.

8.1.1 Amélioration de la sécurité des logiciels des équipements considérés

Les spammeurs peuvent diffuser des spams en utilisant les ressources informatiques ou de réseau qui appartiennent à des tiers une fois que ces ressources présentent des vulnérabilités manifestes. Les ressources ainsi touchées (machines victimes) sont appelées botnets ou ordinateurs zombies. Les spammeurs peuvent contrôler à distance les machines victimes pour envoyer des spams. L'installation d'un système d'exploitation et d'un logiciel d'application sécurisés et la mise à jour en temps utile du logiciel antivirus permettent de protéger efficacement les équipements considérés contre les virus.

8.1.2 Prise en charge de différentes fonctions de gestion

En raison de l'importance des systèmes de service, différentes fonctions de gestion devraient être assurées, dont notamment celles de gestion utilisateur, de gestion système et de gestion d'audit. La fonction de gestion utilisateur est utilisée pour gérer la configuration des gestionnaires, des opérateurs et des "auditeurs". La fonction de gestion système est utilisée pour assurer la maintenance et l'exploitation des équipements. La fonction de gestion d'audit est utilisée pour vérifier les journaux d'opérations et les journaux système. En outre, certains services peuvent nécessiter des fonctions de gestion particulières.

8.1.3 Etablissement de journaux d'opérations et de journaux système

Le système doit établir des journaux d'opérations et des journaux système pour garantir l'exploitation normale du système et maintenir celui-ci dans son état de fonctionnement normal.

Les journaux d'opérations servent à indiquer l'historique des opérations. Tous les événements d'ouverture de session et toutes les opérations établies devraient y être consignés. Les journaux d'opérations devraient inclure au moins les champs suivants: le nom de l'opérateur ainsi que l'heure, la commande et le résultat de l'opération.

Les journaux système peuvent indiquer l'historique de l'état de fonctionnement du système. Celui-ci contient essentiellement des informations sur la qualité de fonctionnement, les pannes, etc. Les données consignées dans les journaux système peuvent varier d'un système à un autre ou d'un service à un autre.

Cela étant, les journaux d'opérations et les journaux système ne sont pas seulement utiles pour la maintenance du système, ils aident également les gestionnaires à garantir des procédures d'exploitation sans activité destructive.

8.1.4 Amélioration de la sécurité et de l'adaptabilité des terminaux

En tant qu'équipements d'utilisateur final les plus importants, les terminaux sont toujours les premières victimes du spam. Etant donné que les fonctions sont toujours différentes d'un type de terminal à un autre, seules des stratégies générales ont pu être déterminées. Ces stratégies sont énumérées, de manière non exhaustive, ci-dessous:

- Prise en charge de l'authentification et de l'autorisation, en particulier pour les terminaux intelligents.
- Prise en charge de listes noires et de listes blanches.
- Installation d'un logiciel antivirus, en particulier pour les terminaux intelligents.

8.2 Stratégies relatives au réseau

A l'instar des stratégies relatives aux équipements, la sécurité du réseau constitue également un élément essentiel dans la lutte contre le spam. Une conception appropriée de la topologie du réseau et la mise en place de divers équipements de sécurité, tels que pare-feux, routeurs sécurisés, passerelles sécurisées, etc., sont de nature à réduire très sensiblement le spam.

8.2.1 Protection des réseaux de services contre les menaces venant de l'Internet

Divers réseaux de services sont confrontés à des menaces émanant de l'Internet du fait que la plupart des services de ces réseaux utilisent des technologies IP avec des normes ouvertes.

Il est nécessaire de prévoir les fonctions suivantes:

- Protection des réseaux de services contre les attaques sur l'Internet, telles que les attaques par déni de service (DoS) et par déni de service réparti (DDoS). Les réseaux de services sont très importants et sont généralement contrôlés à distance par les administrateurs. L'Internet étant ouvert à tous, les réseaux de services devraient pouvoir résister à l'exploitation de vulnérabilités sur l'Internet. Des pare-feux et autres équipements sécurisés sont généralement utilisés pour protéger les réseaux de services contre ces vulnérabilités.
- Protection des signaux de protocole dans le plan de commande pour bloquer les intrusions illicites. Ce point est particulièrement important pour la VoIP. Si le RTPC est toujours sécurisé et fiable, l'Internet n'est ni sécurisé ni fiable. Les passerelles VoIP devraient donc pouvoir bloquer les signaux de protocole illicites afin d'obtenir le même niveau de sécurité que sur le RTPC.

8.2.2 Mise en place d'un mécanisme de redondance et de secours pour maintenir la stabilité du réseau de services

L'importance des équipements et des réseaux de services est telle qu'il convient de prévoir des équipements redondants et des itinéraires de secours. En outre, le mécanisme de redondance et de secours devrait être pratique, efficace et d'un coût raisonnable.

8.3 Stratégies relatives aux services

Les stratégies relatives aux services constituent la partie la plus importante du modèle hiérarchique car les services répondent directement aux besoins des utilisateurs. Mais il faut compter avec de nombreux types de services offrant des fonctions différentes et présentant des vulnérabilités diverses. Les stratégies relatives aux services pour la lutte contre le spam varient donc d'un service à l'autre. Toutefois, les stratégies générales relatives aux services pour la lutte contre le spam sont les mêmes pour les différents services; elles sont indiquées ci-dessous:

8.3.1 Prise en charge de l'authentification

Lorsque des entités (utilisateurs ou équipements) accèdent à des services, une authentification rigoureuse devrait être assurée par les systèmes de service. D'une part, l'authentification rigoureuse empêche les entités non valables d'accéder aux services. D'autre part, les enregistrements d'authentification précis peuvent être utilisés à des fins de traçabilité.

A l'heure actuelle, certains pays ont obtenu des résultats importants sur les réseaux mobiles avec la mise en œuvre de mécanismes d'authentification et de divulgation des vrais noms.

8.3.2 Prise en charge d'adresses de retransmission configurables

Les équipements de service devraient couper la retransmission libre et adopter la retransmission restreinte. Ils devraient prendre en charge des listes d'adresses de retransmission configurables, ne retransmettant que les messages en provenance des adresses autorisées et bloquant les messages en provenance des autres adresses.

8.3.3 Définition rigoureuse du format des messages

Pour certains messages, en particulier les messages commerciaux, le format devrait être défini de manière rigoureuse, les systèmes de service pouvant ainsi obtenir suffisamment d'informations pour traiter les messages.

8.3.4 Compatibilité avec les normes internationales

Afin de renforcer la capacité d'interconnexion et l'interopérabilité, il est demandé que les protocoles de communication des services soient compatibles avec les normes internationales.

8.3.5 Amélioration de la traçabilité des spams

D'une part, les systèmes de service devraient identifier et authentifier les entités (utilisateurs ou équipements) lorsqu'elles accèdent aux systèmes de service, obtenir des informations précises sur ces entités, puis enregistrer les informations pertinentes dans des bases de données. D'autre part, les systèmes de service devraient assurer des fonctions d'audit à des fins de traçabilité, compte tenu des informations consignées dans les bases de données.

8.3.6 Prise en charge du contrôle de flux

Les gestionnaires de systèmes peuvent limiter la largeur de bande de communication ou le nombre de messages transmis durant tout intervalle de temps donné.

8.3.7 Mise en œuvre de fonctions statistiques

Les informations statistiques renseignent les gestionnaires de systèmes sur l'état de leur système à un moment donné (volume de trafic et liste des utilisateurs et des sites consultés, par exemple).

8.4 Stratégies relatives au filtrage

Le filtrage est la technologie antispam la plus courante. Le gros avantage du filtrage réside dans sa simplicité et sa souplesse de mise en œuvre.

8.4.1 Prise en charge du filtrage de spam

On distingue généralement deux types de filtrage: le filtrage par adresse et le filtrage par contenu (dont le filtrage par mot clé).

Le filtrage par adresse peut être utilisé à la fois dans les services avec enregistrement et retransmission et dans les services en temps réel. Pour les services avec enregistrement et retransmission, le filtrage par adresse est utilisé pour filtrer les messages et les courriers électroniques en fonction de l'adresse de leur expéditeur. Ce filtrage est efficace pour empêcher les systèmes de service d'envoyer ou de retransmettre des messages et des courriers électroniques non sollicités (spam). Pour les services en temps réel, le filtrage par adresse est utilisé pour bloquer des appels en fonction des numéros de téléphone ou des adresses des appelants. D'une manière générale, le filtrage par adresse est efficace et pratique pour lutter contre le spam.

Le filtrage par contenu peut aussi être utilisé à la fois dans les services avec enregistrement et retransmission et dans les services en temps réel. Pour les services avec enregistrement et retransmission, le filtrage par contenu est utilisé pour filtrer les messages et les courriers électroniques en fonction des contenus et des mots clés. Pour les services en temps réel, le filtrage par contenu est utilisé pour couper les communications en fonction de leur contenu. En théorie, le filtrage par contenu est plus raisonnable que le filtrage par adresse. Néanmoins, le filtrage par contenu consomme toujours beaucoup de ressources et sa précision est étroitement liée aux algorithmes d'analyse.

Ni l'une ni l'autre de ces deux méthodes de filtrage ne permet de filtrer tous les spams. Il est donc préférable de les utiliser toutes les deux simultanément. En outre, les équipements de service devraient prendre en charge le filtrage des virus.

8.4.2 Mise en œuvre d'un mécanisme de sauvegarde/d'enregistrement pour le filtrage de spam

Pour ce qui est des services avec enregistrement et retransmission, les équipements de service devraient sauvegarder automatiquement les spams. Pour ce qui est des services en temps réel, les équipements de service devraient enregistrer automatiquement les profils des spams. Ces données sont stockées en vue de les consulter ultérieurement, le cas échéant.

8.4.3 Qualité requise pour le filtrage des spams

La qualité est très importante pour le filtrage des spams. Le taux de faux positifs et le taux de faux négatifs sont les facteurs les plus importants pour évaluer la qualité de filtrage des spams. Le terme "faux positifs" désigne les instances négatives détectées en l'absence de toute instance négative, le terme "faux négatifs" désignant quant à lui l'absence d'instances négatives détectées en présence d'instances négatives. Le taux de faux positifs est donc le pourcentage d'instances négatives qui sont signalées à tort comme étant positives. Le taux de faux négatifs est le pourcentage d'instances positives qui sont signalées à tort comme étant négatives. Le Tableau 1 indique le résultat du filtrage des spams.

Tableau 1 – Résultat du filtrage des spams

		Situation concrète	
		Instances positives	**Instances négatives**
Résultat des essais	Instances positives détectées	A	B
	Instances négatives détectées	C	D
NOTE – Les instances positives sont des spams, les instances négatives ne sont pas des spams.			

Le nombre total d'instances soumises aux essais est T.

T = A + B + C + D

B est le nombre de faux positifs.

C est le nombre de faux négatifs.

Taux de faux positifs = B / (B + D).

Taux de faux négatifs = C / (A + C).

Le taux de faux positifs et le taux de faux négatifs sont étroitement corrélés. En règle générale, plus le taux de faux positifs est élevé, plus le taux de faux négatifs est faible. Toutefois, l'importance respective de ces taux variera concrètement en fonction de l'environnement considéré. Dans la pratique commerciale, il est préférable d'accroître le taux de faux négatifs plutôt que le taux de faux positifs.

8.4.4 Mise en place d'une configuration de filtrage souple et ouverte

Devant le nombre et la diversité des spams, il convient de mettre en place une configuration de filtrage souple et ouverte comportant notamment des interfaces faciles à utiliser, des méthodes de configuration sélectionnables, etc. En outre, les règles générales de filtrage peuvent être classées en différentes catégories de filtrage, qui seront répertoriées dans des bases ou référentiels de données. En cas de besoin, ces catégories de filtrage peuvent être sélectionnées et utilisées facilement.

8.4.5 Réduire le plus possible le coût du filtrage

Il est préférable de filtrer le spam le plus tôt possible avant qu'il encombre les systèmes. Le filtrage du spam devrait donc être assuré en début de transmission et non pas par les équipements de service ultérieurs.

8.4.6 Prise en charge de listes noires et de listes blanches

On distingue deux types de filtrage par adresse: les listes blanches ou listes des expéditeurs autorisés, et les listes noires ou listes des spammeurs présumés.

Les listes noires sont établies d'après le listage des expéditeurs de spams. Ce listage peut comporter les noms des machines, les adresses IP, les adresses MAC ou d'autres types d'adresses électroniques. Le système de filtrage peut filtrer les messages ou bloquer les communications d'après les listes noires.

Les listes blanches sont établies d'après le listage des expéditeurs autorisés. Le mécanisme de fonctionnement est analogue à celui des listes noires, à ceci près que les listes blanches énumèrent les adresses autorisées.

Dans la pratique, la solution des listes blanches/listes noires est généralement trop grossière pour pouvoir être acceptée par la plupart des utilisateurs. Toutefois, il s'agit là de solutions très simples et qui ne nécessitent pas beaucoup de ressources. Afin d'améliorer l'efficacité du filtrage, des filtres devraient prendre en charge des listes blanches et des listes noires, surtout des listes noires pour lutter contre le spam.

8.4.7 Prise en charge du filtrage des messages multimodaux

Pour les messages multimodaux, il est nécessaire de:

- prendre en charge la capacité de bloquer entièrement certains messages multimodaux;
- prendre en charge la capacité de supprimer certaines pièces jointes de messages multimodaux ou certains contenus multimodaux partiels d'un message multimédia;
- prendre en charge la capacité de filtrer les messages multimodaux entrants (reçus) et/ou sortants (envoyés).

8.5 Stratégies relatives au retour de l'information

Les utilisateurs finals sont les destinataires finals du spam, les victimes possibles de virus et de scams. La participation des utilisateurs finals sera utile pour lutter efficacement et rationnellement contre le spam. Les réactions des utilisateurs finals devraient donc être prises en considération pour la mise au point de solutions de lutte contre le spam. Toutefois, la participation de l'utilisateur final au mécanisme de retour de l'information devrait se faire sur la base du volontariat.

8.5.1 Mise en place d'une plate-forme de collecte des réactions au spam

Les particuliers victimes de spams préjudiciables devraient pouvoir introduire des recours. Les droits des personnes physiques, en tant que destinataires de spams, doivent être protégés par la législation. Des moyens de recours doivent donc être mis à leur disposition. Des mécanismes doivent être établis à cet effet, indiquant notamment la procédure à suivre pour signaler à une autorité compétente toute atteinte à un droit par voie de spam. De telles procédures de traitement des réactions doivent être transparentes, efficaces et rationnelles. Une plate-forme de collecte des réactions peut répondre à ce triple objectif.

8.5.2 Adoption d'un format normalisé pour la mise en commun des réactions

Pour que la plate-forme de collecte des réactions puisse remplir correctement sa mission, l'adoption d'un format d'enregistrement normalisé s'impose. Ce format permettra aux différents opérateurs et entités de mettre en commun les réactions qu'ils auront recueillies. Cette confrontation des réactions permettra d'obtenir les principales adresses des spammeurs, qui pourront être incluses dans les listes noires.

9 Evaluation des systèmes

Afin d'évaluer le bon fonctionnement et l'efficacité des technologies et des systèmes de lutte contre le spam, il convient de prendre en considération les éléments suivants:

- Taux de faux positifs.
- Taux de faux négatifs.
- Coût: les méthodes de lutte contre le spam devraient être souples et ouvertes pour permettre la mise au point de solutions adaptées aux besoins des utilisateurs. En raison du grand nombre de combinaisons possibles de stratégies, il est souhaitable de disposer de profils qui couvrent une large gamme de services.
- Interopérabilité des systèmes actuels: la garantie du fonctionnement normal des systèmes actuels constitue la condition sine qua non de la lutte contre le spam. En d'autres termes, la mise en œuvre des solutions de lutte contre le spam ne saurait perturber le fonctionnement des systèmes actuels.

- Conformité aux normes internationales: les solutions techniques devraient de préférence être axées sur les normes internationales pour assurer l'interconnexion et le développement à l'échelle planétaire. En outre, la normalisation facilitera la réutilisation des solutions et des composants, ce qui rendra possible la mise en œuvre rapide et à bas coût de nouvelles solutions et techniques de lutte contre le spam.

Les éléments susmentionnés constituent des critères généraux pour évaluer les mesures de lutte contre le spam. Dans la pratique, d'autres éléments concrets seront à prendre en considération dans les réseaux de services.

Bibliographie

[b-UIT-T Q.1742.3] Recommandation UIT-T Q.1742.3 (2004), *Références IMT-2000 (approuvées au 30 juin 2003) au réseau central évolué ANSI-41 avec réseau d'accès cdma2000.*

[b-UIT-T Q-Sup.49] Supplément 49 aux Recommandations UIT-T de la série Q (2004), *Rapport technique TRQ.2840: Prescriptions de signalisation pour la prise en charge de la téléphonie IP*.

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

[b-UIT-T X.811] Recommandation UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'authentification.*

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs.* <http://www.ietf.org/rfc/rfc2505.txt>

[b-IETF RFC 2554] IETF RFC 2554 (1999), *SMTP Service Extension for Authentication.* <http://www.ietf.org/rfc/rfc2554.txt>

[b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*).* <http://www.ietf.org/rfc/rfc2635.txt>

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol.* <http://www.ietf.org/rfc/rfc2821.txt>

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions.* <http://www.ietf.org/rfc/rfc3685.txt>

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
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
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

Imprimé en Suisse
Genève, 2009