Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1247

Amendement 1

(05/2022)

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

Sécurité du cyberespace – Lutte contre le spam

Cadre technique de lutte contre le spam par messagerie mobile

Amendement 1

Recommandation UIT-T X.1247 (2016) – Amendement 1

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 (1)	
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 (1)	X.1140–X.1149
Sécurité des applications (1)	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
Lutte contre le spam	**X.1230–X.1249**
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1350–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1399
Sécurité de la technologie des registres distribués (DLT)	X.1400–X.1429
Sécurité des applications (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470–X.1489
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
Cyberdéfense	X.1590–X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
Protection des données	X.1770–X.1789
SÉCURITÉ DES IMT-2020	X.1800–X.1819

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

Recommandation UIT-T X.1247

Cadre technique de lutte contre le spam par messagerie mobile

Amendement 1

Résumé

Le phénomène du spam par messagerie mobile connaît un essor spectaculaire en raison du développement rapide des services de messagerie mobile. Malheureusement, aucune mesure ne s'est avérée à ce jour efficace pour remédier à ce problème, d'où la nécessité de mettre en place un cadre pratique de lutte contre le spam par messagerie mobile. La Recommandation UIT-T X.1247 donne un aperçu des méthodes de lutte contre le spam par messagerie mobile et propose un cadre technique de lutte contre ce phénomène. Ce cadre définit les fonctions incombant aux entités et les procédures de traitement à suivre. En outre, cette Recommandation décrit des mécanismes d'échange d'informations pour lutter contre le spam par messagerie mobile dans le domaine du traitement antispam ou entre plusieurs domaines de traitement antispam.

L'amendement 1 présente le mécanisme de retour d'information du client, qui reçoit éventuellement un appel non sollicité (par service vocal, par service de messages courts (SMS) ou par service de messagerie multimédia (MMS)), à son opérateur. Il décrit les exigences techniques relatives aux systèmes de gestion des télécommunications et/ou services d'assistance aux clients pour recevoir des notifications relatives aux appels entrants non sollicités, par service vocal ou messagerie (SMS ou MMS). Il présente également des scénarios d'interaction entre les clients et les opérateurs ou fournisseurs de services des réseaux de communication téléphonique concernant des appels entrants non sollicités de même que les mesures techniques à appliquer dans ce cadre. Cette interaction suppose que le destinataire de l'appel non sollicité passe un appel au numéro anti-spam fourni au préalable par l'opérateur de télécommunication immédiatement après avoir reçu l'appel non sollicité.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1247	23-03-2016	17	11.1002/1000/12600
1.1	UIT-T X.1247 (2016) Amd. 1	20-05-2022	17	11.1002/1000/14989

Mots clés

Antispam, spam par messagerie mobile, cadre technique.

---

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

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.

À 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 ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise 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 les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Page

Introduction

Le service de messagerie mobile, y compris le service de messages courts et le service de messagerie multimédia, connaît un essor très rapide, ce service étant peu coûteux et facile à utiliser et offrant une grande souplesse. Cependant, le spam par messagerie mobile est à l'origine de désagréments dans la vie quotidienne des usagers et a de nombreuses conséquences négatives.

On peut difficilement remédier efficacement au problème du spam par messagerie mobile en n'ayant recours qu'à une seule solution. L'utilisation de techniques de lutte contre le spam dans le cadre d'une coopération permet d'atténuer sensiblement le préjudice causé par le spam par messagerie mobile. En outre, étant donné que le spam par messagerie mobile est un phénomène qui s'est généralisé dans le monde entier, une coopération entre plusieurs domaines de traitement antispam permet de fournir le service de façon beaucoup plus efficace et économique. En conséquence, il est nécessaire d'établir un cadre ouvert qui prenne en considération diverses solutions et prévoie plusieurs mécanismes de collaboration. Ce cadre est compatible avec la plupart des techniques de lutte contre le spam et ne se limite pas à des détails techniques particuliers. Les procédures concernées dans ce cadre doivent faire l'objet d'un accord exprès de la part de l'utilisateur final du dispositif mobile et être conformes aux réglementations ainsi qu'aux législations nationales.

Recommandation UIT-T X.1247

Cadre technique de lutte contre le spam par messagerie mobile

Amendement 1

Note rédactionnelle: La présente publication contient le texte intégral de la Recommandation. Les modifications introduites par le présent amendement sont indiquées par des marques de révision apportées à la Recommandation UIT-T X.1247 (2016).

1 Domaine d'application

La présente Recommandation fixe un cadre technique pour la lutte contre le spam par messagerie mobile. Ce cadre décrit les fonctions exercées par les entités et les procédures de traitement à suivre. Les procédures concernées dans ce cadre doivent faire l'objet d'un accord exprès de la part de l'utilisateur final du dispositif mobile et être conformes aux réglementations ainsi qu'aux législations nationales. En outre, la présente Recommandation décrit des mécanismes d'échange d'informations pour lutter contre le spam par messagerie mobile dans le domaine du traitement antispam ou entre plusieurs domaines de traitement antispam.

La présente Recommandation est applicable au service de messages courts (SMS) et au service de messagerie multimédia (MMS).

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

~~Aucune.~~[UIT-T X.1246] Recommandation UIT-T X.1246 (2015), *Technologies intervenant dans la lutte contre le spam vocal dans les organisations de télécommunication*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 numéro anti-spam [UIT-T X.1246]: numéro de téléphone spécial prédéfini par le fournisseur de services/l'opérateur de télécommunication national/propre (ce numéro peut être unique sur le territoire national ou spécifique à chaque opérateur), en appelant ce que l'utilisateur notifie d'un appel spam sur son numéro de téléphone directement avant d'appeler ce numéro anti-spam. La notification, c'est le fait d'appeler le numéro anti-spam; l'utilisateur ne doit fournir aucune information.

3.1.2 rapport d'utilisateur interactif [UIT-T X.1246]: plainte d'un abonné qui reçoit un message téléphonique contenant un spam ou qui est lui-même un spam. En règle générale, le rapport concerne l'appel (ou plutôt les circonstances de l'appel) passé à un numéro anti-spam ou l'acheminement d'un appel non sollicité suspect avec un message vers un numéro anti-spam.

3.1.~~1~~3 spam par SMS [b-UIT-T X.1242]: spam envoyé par SMS.

3.1.~~2~~4 spam [b-UIT-T X.1240]: le sens du mot "spam" dépend de la perception du respect de la vie privée et de ce que constitue le spam au niveau de chaque pays, du point de vue technologique, économique, social et pratique. En particulier, ce sens évolue et se diversifie au fur et à mesure du développement des technologies, donnant lieu à de nouvelles possibilités d'utilisation abusive des communications électroniques. Bien qu'aucune définition du spam n'ait été adoptée à l'échelle mondiale, ce terme est couramment employé pour décrire des communications électroniques de masse non sollicitées transmises par courrier électronique (courriel) ou par messagerie mobile pour promouvoir des produits ou services commerciaux.

3.1.5 appel non sollicité [UIT-T X.1246]: appel téléphonique contenant un message vocal, texte ou multimédia non sollicité et visant généralement à faire de la publicité de produits ou services commerciaux.

3.1.~~3~~6 spammeur [b-UIT-T X.1240]: entité ou personne qui crée et envoie des spams.

3.1.7 appel non sollicité suspect [UIT-T X.1246]: appel téléphonique indéterminé soupçonné d'être un spam.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 domaine antispam: système indépendant comprenant une fonction de gestion antispam, une fonction de contrôle antispam, une fonction de traitement antispam et un client de messagerie mobile.

NOTE – Les fonctions du domaine antispam sont subordonnées à la gestion unifiée de l'opérateur.

3.2.2 entité de filtrage antispam: équipements ou systèmes qui prennent des mesures antispam pour filtrer les messages sur mobile en fonction de règles de filtrage. Ces équipements ou systèmes peuvent bloquer les spams, signaler les messages considérés comme suspects ou envoyer des messages au destinataire.

3.2.3 fonctions de gestion antispam: groupe de fonctions utilisées pour gérer et superviser le domaine antispam, notamment la communication avec d'autres domaines antispam, pour l'échange d'informations sur les spams, la création de nouvelles règles de filtrage à partir d'une analyse des spams et la diffusion de ces règles aux fonctions de traitement antispam.

3.2.4 fonctions de contrôle antispam: groupe de fonctions utilisées pour contrôler et analyser les résultats du filtrage du domaine de traitement antispam, notamment la validation des spams suspects détectés par la méthode du leurre, l'analyse des données concernant les spams, l'établissement de statistiques concernant les spams et les résultats de l'analyse des spams.

3.2.5 fonctions de traitement antispam: groupe de fonctions utilisées pour traiter les messages mobiles à l'aide de règles et de politiques de filtrage. Ces fonctions permettent de traiter les messages en bloquant les spams, en envoyant des messages avec une indication spéciale ou en envoyant des messages au destinataire.

3.2.6 faux négatif: un spam par messagerie mobile a été traité par erreur en tant que message autre qu'un spam par le système de filtrage.

3.2.7 faux positif: un message a été identifié par erreur comme étant un spam par le système de filtrage.

3.2.8 règles de filtrage: série de règles d'algorithmes de comptage mises en place par l'entité de filtrage antispam, par exemple des listes noires/listes blanches, un seuil de similitude et un seuil statistique. Les règles de filtrage peuvent également comprendre des règles de filtrage définies par l'utilisateur.

3.2.9 client de messagerie mobile: abonné au service de messagerie mobile.

3.2.10 spam par messagerie mobile: communications électroniques non sollicitées transmises par les services de messagerie mobile et comprenant généralement des spams acheminés par le service de messages courts (SMS) et le service de messagerie multimédia (MMS).

3.2.11 spam acheminé par le service de messagerie multimédia (MMS): spam envoyé par MMS.

3.2.12 service de notification: service assurant la collecte et le regroupement des rapports de l'abonné sur les spams, avec l'autorisation de l'utilisateur et conformément aux réglementations et aux législations nationales.

3.2.13 rapport d'analyse des spams: le résultat analysé indique l'efficacité du système de filtrage. Il devrait comprendre le taux de faux positifs/faux négatifs du filtrage, les caractéristiques du spam de messagerie, l'évolution du spam et d'autres analyses.

3.2.14 statistiques sur le spam: les données agrégées sur le spam indiquent l'ampleur du spam dans certaines conditions de contrainte, par exemple un intervalle de temps dans un domaine antispam. Ces statistiques devraient comprendre la quantité de spams par messagerie à l'intérieur d'un domaine, entrant dans un domaine ou quittant un domaine, la proportion des différents types de spam, la liste de spammeurs et d'autres données statistiques sur les spams.

3.2.15 spam suspect: message mobile indéterminé soupçonné d'être un spam.

3.2.16 rapport de l'utilisateur: plainte d'un abonné qui reçoit un spam par messagerie mobile. En général, ce rapport peut indiquer la date de réception du spam, le numéro international du réseau numérique à intégration de services/réseau téléphonique public commuté (RNIS/RTPC) de l'abonné mobile (MSISDN) de l'expéditeur et du destinataire, etc. Ce rapport donne également des renseignements sur les messages signalés par erreur comme étant des spams mobiles, ou non signalés comme étant des spams, alors qu'ils auraient dû l'être, c'est-à-dire le nombre de faux positifs et de faux négatifs.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AMgmt	fonction de gestion de messagerie mobile antispam (*anti-spam mobile messaging management function*)
Amon	fonction de contrôle de messagerie mobile antispam (*anti-spam mobile messaging monitoring function*)
AO	lancé par l'application (*application originated*)
APr	fonction de traitement de messagerie mobile antispam (*anti-spam mobile messaging processing function*)
Caller ID	identification de l'appelant (*caller identification*)
CDR	relevé détaillé de l'appel (*call detail record*)
CDR_n	relevé détaillé de l'appel initial (*initial call detail record*)
CDR_{n+1}	relevé détaillé de l'appel interactif renvoyé par l'utilisateur à son opérateur (*interactive call detail record back from the user to its operator*)
CLI	identification de la ligne appelante (*calling line identification*)
CLI_n	identification de la ligne appelante de l'appelant initial à l'utilisateur (*calling line identification of initial caller to the user*)
CLI_{n+1}	identification de la ligne appelante de l'utilisateur, lorsqu'il passe un appel de retour d'information sur un numéro anti-spam (*calling line Identification of the user, when it makes a feedback call to an anti-spam number*)

GGSN	nœud de support du service GPRS de transit (*gateway GPRS supporting node*)
GPRS	service général de radiocommunication en mode paquet (*general packet radio service*)
HTTP	protocole de transfert hypertexte (*hypertext transfer protocol*)
MAP	sous-système application mobile (*mobile application part*)
MMS	service de messagerie multimédia (*multimedia messag~~e~~ing service*)
MMSC	centre du service de messagerie multimédia (*multimedia messag~~e~~ing service centre*)
MNO	opérateur de réseau mobile (*mobile network operator*)
MO	orienté mobile (*mobile oriented*)
MSC	centre de commutation pour les services mobiles (*mobile switching centre*)
MSISDN	numéro international RNIS/RTCP de l'abonné mobile (*mobile subscriber international ISDN/PSTN number*)
MT	à destination d'un mobile (*mobile terminated*)
QoS	qualité de service (*quality of service*)
RMTP de rattachement	réseau mobile terrestre public de rattachement
RMTP visité	réseau mobile terrestre public visité
RNIS	réseau numérique à intégration de services
RTPC	réseau téléphonique public commuté
SMPP	messages courts entre homologues (*short message peer-to-peer*)
SMS	service de messages courts (*short message service*)
SMSC	centre du service de messages courts (*short message service centre*)
UICC	carte à circuit intégré universelle (*universal integrated circuit card*)
WAP	protocole d'application sans fil (*wireless application protocol*)

5 Conventions

Aucune.

6 Vue d'ensemble de la messagerie mobile antispam

Comme indiqué sur la Figure 6-1, il existe pour l'essentiel deux moyens de créer un spam dans le service de messages courts (SMS): le premier consiste pour les spammeurs à utiliser des outils spam pour diffuser massivement des messages, en envoyant des messages courts normaux point à point à l'aide de nombreuses cartes à circuit intégré universelles (UICC) acquises ou dupliquées, tandis que le second consiste, pour les spammeurs, à avoir recours aux services d'expédition de messages en masse offerts par les fournisseurs de services en utilisant les interfaces passerelles pour les messages courts de l'opérateur. Étant donné que les opérateurs ne disposent d'aucun mécanisme efficace de supervision technique et de gestion de l'interface passerelle pour les messages courts, celle-ci peut aisément être utilisée par les spammeurs.

En fonction du sens de retransmission des messages, il existe deux procédures permettant aux spammeurs de créer un spam par SMS, appelées procédure orientée mobile (MO)/procédure lancée par l'application (AO) et procédure à destination d'un mobile (MT). Avec la procédure MO, le spam

créé par des outils spam est envoyé au centre du service de messages courts (SMSC) par l'intermédiaire des entités correspondantes du réseau de l'expéditeur. Avec la procédure AO, le message court injecté dans le spam depuis la passerelle de messages courts de l'opérateur est retransmise au centre SMSC. Par la suite, le centre SMSC interroge le centre de commutation mobile (MSC) desservant les destinataires, puis lui transmet le message. Enfin, le message court est transmis au destinataire par l'intermédiaire du réseau visiteur du MSC, ce qui correspond à la procédure MT.

À condition d'y être autorisé par l'abonné et par les réglementations administratives applicables, les opérateurs de réseaux mobiles (MNO) sont habilités à limiter les spams par messagerie en ayant recours à des entités de filtrage. Le processus antispam doit être rigoureusement conforme aux dispositions de la législation applicable, afin de ne pas enfreindre le droit à la vie privée de l'abonné.

La pratique consistant à déployer des entités de filtrage antispam dans la procédure MO/AO, la procédure MT, ou une combinaison de ces deux procédures, est largement répandue. Pour le filtrage des spams selon la procédure MO, les entités de filtrage antispam recueillent des messages courts auprès du centre SMSC. Afin que filtrage des spams soit efficace au niveau du réseau du destinataire, une communication entre le MSC et l'entité de filtrage antispam est également nécessaire.

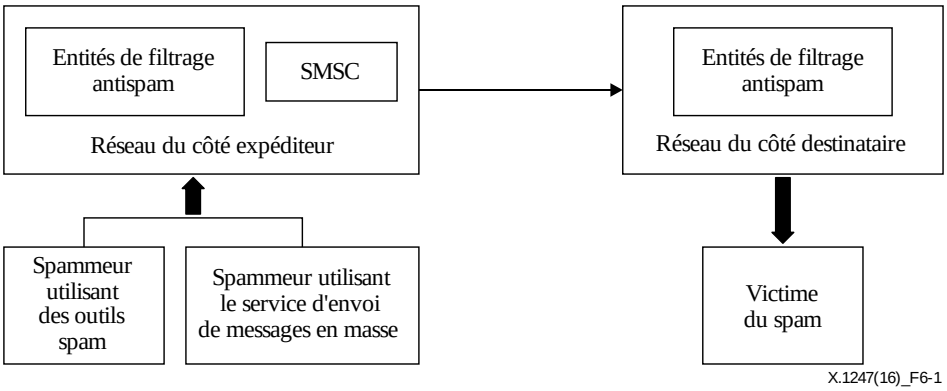

Figure 6-1 – Spam par SMS dans le réseau mobile

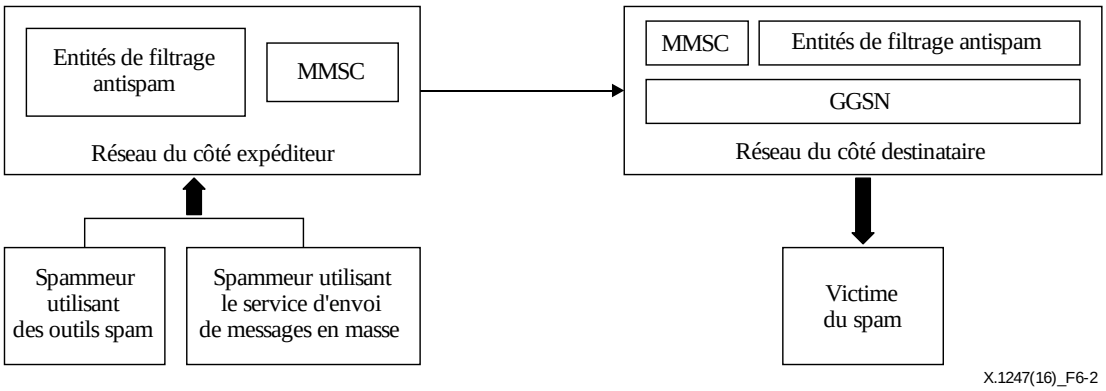

Figure 6-2 – Spam par MMS dans le réseau mobile

Comme indiqué sur la Figure 6-2, la procédure de messagerie du service de messagerie multimédia (MMS) est analogue à celle applicable au SMS, si ce n'est que le MSC est remplacé par le nœud de support du service GPRS de transit (GGSN) et que le SMSC est remplacé par le centre du service de messagerie multimédia (MMSC). Le message MMS sera transmis au centre MMSC du réseau du destinataire, après quoi le centre SMSC enverra un message SMS au destinataire. Celui-ci téléchargera alors le message MMS depuis le centre MMSC. C'est pourquoi il est possible de déployer

des entités de filtrage antispam MMS à proximité du centre MMSC, ce qui signifie que les entités de filtrage peuvent être déployées indifféremment du côté de l'expéditeur, ou du côté du destinataire.

7 Structure des fonctions de messagerie mobile antispam

La structure des fonctions de messagerie mobile antispam comprend la fonction de gestion de messagerie mobile antispam (AMgmt), la fonction de contrôle de messagerie mobile antispam (AMon), la fonction de traitement de messagerie mobile antispam (APr) et les clients de la messagerie mobile. Ces fonctions définissent le domaine de messagerie mobile antispam.

Il est recommandé d'associer différents domaines de messagerie mobile antispam, de façon qu'ils puissent se concerter en fonction des règles ou politiques définies par les accords pertinents.

Ces fonctions peuvent communiquer entre elles par le biais des protocoles de messagerie existants et leurs caractéristiques sont décrites ci-dessous.

7.1 Structure générale

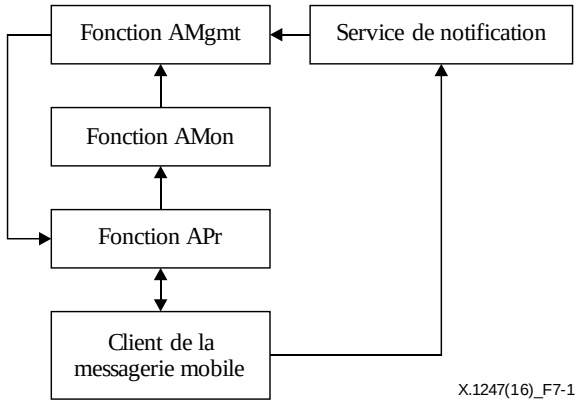

Figure 7-1 – Structure générale

La fonction AMgmt reçoit de la fonction AMon des statistiques sur le spam et met à jour les règles de filtrage relevant de son domaine. La fonction AMgmt échange également des informations sur le spam avec le service de notification et les autres fonctions AMgmt.

La fonction AMon reçoit de la fonction APr des spams de messagerie mobile suspects, qui sont saisis par une méthode de leurre ou à l'aide de plates-formes analogues, et vérifie qu'il s'agit de spams. La fonction AMon transmet également l'analyse des spams et les statistiques relatives aux spams à la fonction AMgmt après avoir rassemblé et analysé les données relatives aux spams.

La fonction APr applique les règles aux messages mobiles, puis choisit de les envoyer avec indication qu'il s'agit de spams, ou de les bloquer, en fonction des différentes politiques et des résultats du filtrage autorisé par l'utilisateur. La fonction APr reçoit de la fonction AMgmt les règles de filtrage et les commentaires des utilisateurs fournis par les clients de la messagerie mobile. Il est recommandé de déployer un certain nombre de plates-formes, par exemple un leurre, sur la fonction APr, afin de rassembler les spams suspects.

Le client de la messagerie mobile contribue au processus de messagerie mobile antispam lorsque l'utilisateur envoie en retour des commentaires selon lesquels le message mobile reçu indiqué comme étant un spam est incorrect pour la fonction APr et envoie un rapport de spam au service de notification.

Le service de notification a pour objet de recueillir et de rassembler les rapports des abonnés sur les spams, avec l'autorisation de l'utilisateur et conformément aux réglementations ainsi qu'aux

législations nationales. Ce service contribue à l'échange des données figurant dans les rapports des utilisateurs entre domaines de traitement antispam. Le service de notification pourra être géré par une instance de régulation, une entreprise de sécurité ou un opérateur MNO, etc. Les accords interdomaines permettent aux domaines de messagerie mobile antispam d'échanger des informations personnalisées sur le spam.

7.2 Modèle de référence

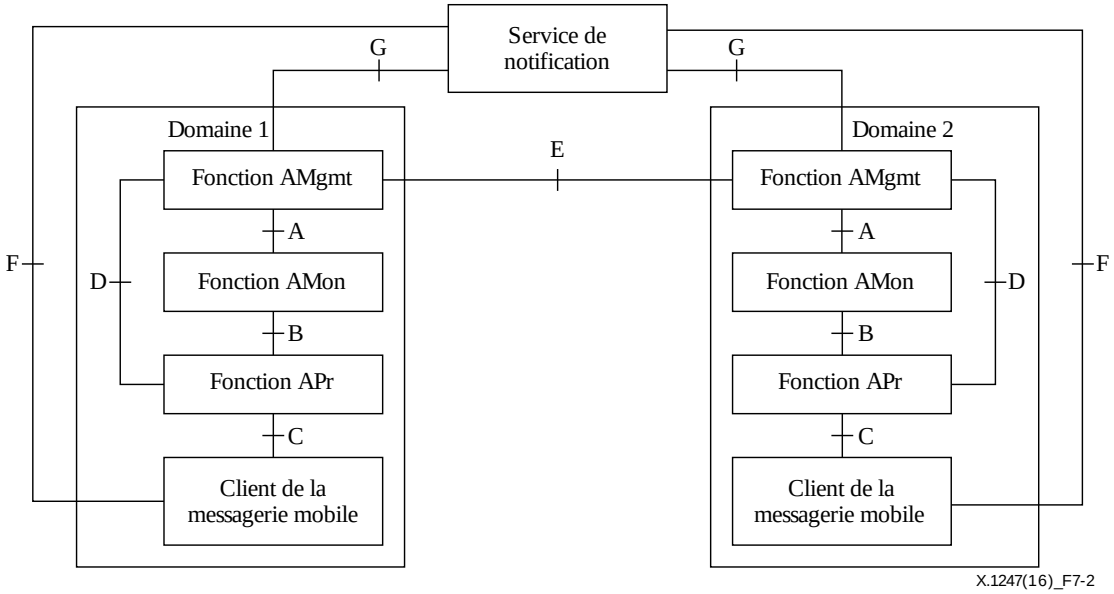

Figure 7-2 – Modèle de référence

L'interface A est une interface logique entre les fonctions AMgmt et AMon. Elle est utilisée pour transmettre les rapports sur l'analyse des spams et les statistiques relatives aux spams.

L'interface B est une interface logique entre les fonctions AMon et APr. Elle est utilisée pour transmettre les spams suspects repérés à l'aide de la méthode du leurre et grâce aux commentaires des utilisateurs selon lesquels le message mobile reçu de la part du client de la messagerie mobile et signalé comme étant un spam est incorrect.

L'interface C est une interface logique entre la fonction Apr et le client de la messagerie mobile. Elle est utilisée par le client de la messagerie mobile pour informer la fonction APr qu'un message reçu a été signalé à tort comme étant un spam par un opérateur MNO. En outre, l'interface C sert à envoyer des messages de la fonction APr vers le client de la messagerie mobile. En fonction des différents types de clients de la messagerie mobile, il convient de prendre en charge différents protocoles au niveau de l'interface C, par exemple le sous-système application mobile et le protocole d'application sans fil (MAP/WAP), le protocole de transfert hypertexte (HTTP) et les messages courts entre homologues (SMPP).

L'interface D est une interface logique entre les fonctions AMgmt et APr. Elle est utilisée pour transmettre les règles de filtrage.

L'interface E est une interface logique entre les fonctions AMgmt et d'autres domaines. Elle est utilisée pour échanger des données relatives aux spams entre différents domaines de messagerie mobile antispam.

L'interface F est une interface logique entre le client de la messagerie mobile et le service de notification. Elle est utilisée par le client de la messagerie mobile pour envoyer un rapport de l'utilisateur au service de notification avec l'accord exprès de l'utilisateur. Il convient de prendre en charge différents protocoles au niveau de l'interface F, par exemple le sous-système application

mobile et le protocole d'application sans fil (MAP/WAP), le protocole de transfert hypertexte (HTTP) et les messages courts entre homologues (SMPP).

L'interface G est une interface logique entre la fonction AMgmt et le service de notification. Elle a pour but de transmettre les informations figurant dans le rapport sur les spams du service de notification vers la fonction AMgmt.

Dans ce modèle de référence, les interfaces A à D sont des interfaces intradomaine, tandis que les interfaces E à G sont des interfaces interdomaines.

7.3 Fonctions des composantes

7.3.1 Clients de la messagerie mobile

Les fonctions du client de la messagerie mobile consistent:

- à fournir des mécanismes destinés à aider les utilisateurs à envoyer des rapports d'utilisateur au service de notification;
- à fournir des mécanismes destinés à aider les utilisateurs à informer la fonction APr de la réception de messages signalés par erreur comme étant des spams;
- à filtrer les messages au moyen de règles de filtrage spéciales utilisant des applications de sécurité.

7.3.2 Fonction APr

Les fonctions APr consistent:

- à appliquer les règles de lutte contre le spam fournies par la fonction AMgmt et à choisir d'envoyer, d'envoyer avec indication que le message est suspect ou de bloquer le message en fonction des différentes politiques et du résultat du filtrage;
- à recevoir les commentaires de l'utilisateur provenant du client de la messagerie mobile, selon lesquels le message mobile reçu, signalé comme étant un spam, n'en est pas un;
- à recueillir le spam suspect à l'aide de la méthode du leurre ou d'autres plates-formes analogues;
- à remettre les commentaires de l'utilisateur ainsi que le spam suspect recueilli à l'aide de la méthode du leurre à la fonction AMon.

7.3.3 Fonction AMon

Les fonctions AMon consistent:

- à rassembler les spams suspects recueillis à l'aide de la méthode du leurre auprès de la fonction APr ainsi que les renseignements contenus dans le rapport de l'utilisateur auprès du service de notification;
- à valider le spam suspect provenant de la fonction APr;
- à analyser les données agrégées relatives aux spams afin d'analyser les caractéristiques des nouveaux spams;
- à faire rapport sur les statistiques et l'analyse relatives aux spams à la fonction AMgmt.

7.3.4 Fonction AMgmt

Les fonctions AMgmt consistent:

- à recevoir les statistiques et le rapport d'analyse sur les spams de la fonction AMon;
- à analyser les données communiquées par la fonction AMon pour créer des règles de filtrage;
- à envoyer les règles de filtrage à la fonction APr, après quoi ces règles seront appliquées aux clients de la messagerie mobile;

- à communiquer avec les autres fonctions AMgmt pour échanger et partager des données relatives aux spams, telles que la quantité de spams, les ressources et les caractéristiques des spams, la liste des nouveaux spammeurs, etc.;
- à recevoir les informations contenues dans le rapport de l'utilisateur fourni par le service de notification, notamment les abus les plus graves en matière de spam, ainsi que les statistiques et les tendances relatives aux spams. Les informations contenues dans le rapport de l'utilisateur peuvent être personnalisées et comprennent certaines données traitées provenant du rapport de l'utilisateur, en fonction de l'accord conclu avec le service de notification dans les limites autorisées par les réglementations et législations nationales;
- à permettre à l'abonné de fixer des règles de filtrage propres à l'utilisateur et à envoyer ces règles à la fonction APr après en avoir vérifié la validité.

7.3.5 Service de notification

Les fonctions du service de notification consistent:

- à recueillir les rapports des utilisateurs et à vérifier qu'il s'agit de spams;
- à stocker et à analyser les spams, afin de définir les caractéristiques des spams et d'utiliser des empreintes et non pas des contenus, de façon à éviter toute violation du droit au respect de la vie privée;
- à fournir les données contenues dans le rapport de l'utilisateur, pour permettre à l'opérateur MNO de mieux cerner le volume de spams à l'intérieur de leur réseau, entrant dans leur réseau ou quittant leur réseau en provenance d'autres opérateurs, qui ont demandé aux opérateurs MNO d'utiliser cette visibilité pour cibler les mesures répressives à prendre à l'encontre des auteurs de spam par messagerie mobile uniquement, sans que cela n'ait d'incidence pour les utilisateurs et le contenu.

8 Techniques de lutte contre le spam par messagerie mobile

Les techniques exposées dans le présent paragraphe s'appliquent à la structure antispam décrite ci-dessus et sont fournies à titre d'exemple. Toutes ces mesures doivent être utilisées avec le plus grand soin, afin d'être conformes à la réglementation et aux législations nationales applicables et avec l'autorisation de l'utilisateur, de façon à éviter toute violation du droit au respect de la vie privée de l'utilisateur.

8.1 Mécanismes pour le traitement des commentaires des utilisateurs

Les mécanismes pour le traitement des commentaires des utilisateurs permettent aux abonnés de faire connaître au système de filtrage leurs points de vue sur les résultats du filtrage des spams. Il est recommandé de mettre en place un service de notification et de présentation des commentaires des utilisateurs pour améliorer les résultats du filtrage effectué par l'opérateur MNO.

Un service de notifications est un système visant à recueillir les rapports des utilisateurs sur les messages spam reçus, qui peut être mis en place par les gouvernements, les opérateurs, etc. Le service de notification peut être une ligne d'assistance, un site web ou un centre de notification de spam par messages courts, afin que l'opérateur MNO puisse recueillir les spams par messages courts et ajuster les règles de filtrage. En général, le dossier de la réclamation concernant les spams par messages courts devrait comprendre la valeur de hachage du message spam, l'heure de réception ainsi que le numéro MSISDN de l'expéditeur, etc. En fonction des différentes politiques et uniquement si l'utilisateur a donné son accord, l'opérateur MNO peut non seulement bloquer le spam, mais aussi donner au destinataire un accès à une quarantaine, ce qui signifie que ces messages pourront être envoyés avec une indication, ou être enregistrés dans un site web donné. Cela permet aux destinataires de visualiser ces "spam potentiels", qui ont été signalés comme spams suspects, et de formuler leurs commentaires s'ils considèrent qu'une décision sur tel ou tel message est incorrecte ou correspond à

un "faux positif". Les commentaires des utilisateurs ne sont pas tous fiables en soi. Les destinataires peuvent commettre des erreurs ou avoir d'autres raisons de signaler des messages comme étant des spams. Il faut vérifier manuellement les renseignements permettant de reconnaître un spam, avant de les utiliser pour créer des empreintes ou des règles de filtrage. La mise au point d'un système d'évaluation de la confiance de l'auteur du signalement est possible, afin de différencier automatiquement les commentaires valables des commentaires erronés ou malveillants.

8.2 Leurre

Un leurre par numéro de téléphone est un compte créé sous la forme d'un "piège", pour détecter, transférer ou empêcher l'utilisation non autorisée de messages sur mobile. Il s'agit généralement d'un compte qui est utilisé ou créé en vue d'être découvert par des spammeurs, englobant les numéros de téléphone inactifs ou inexistants. Ainsi, tout message qui est différent de ce qui est prévu peut être considéré comme un spam suspect et il conviendra peut-être d'en analyser le contenu. Les numéros de téléphone peuvent être réattribués rapidement et sont souvent saisis de façon incorrecte, de sorte que les leurres par numéro de téléphone recevront de nombreux messages de type accidentel ou de messages autres que des spams. Il est nécessaire de vérifier ces spams suspects, afin de filtrer ces données non sollicitées avant d'analyser le spam suspect pour en déterminer les caractéristiques.

La présentation des commentaires des utilisateurs subit parfois des retards, étant donné qu'il peut s'écouler plusieurs minutes ou plusieurs jours avant qu'un message non sollicité ne soit signalé par les destinataires. En revanche, les pièges par leurre peuvent détecter des messages indésirables dès qu'ils sont remis.

8.3 Méthode d'identification par les opérateurs MNO

Exception faite des commentaires des utilisateurs et des leurres, les opérateurs MNO peuvent prendre d'autres mesures pour repérer les spams avant de les envoyer aux destinataires. En mettant en œuvre différentes politiques, ils bloqueront ces messages ou les enverront avec une indication spéciale selon laquelle il s'agit de messages suspects. Ces méthodes d'identification pourront dépendre des caractéristiques du spam ou de la configuration de l'envoi.

- Liste noire/liste blanche de numéros internationaux du réseau numérique à intégration de services/réseau téléphonique public commuté (RNIS/RTPC) (MSISDN).

  Les numéros MSISDN constituent les principaux renseignements qui permettent de distinguer un message provenant d'un abonné d'un message provenant d'un spammeur. Les listes noires/listes blanches utilisent le numéro MSISDN de l'expéditeur pour suspendre/accepter des messages. Les opérateurs mobiles pourront bloquer les spammeurs connus ou reconnus, tandis que les abonnés pourront définir leurs propres listes noires/listes blanches pour bloquer ou accepter des messages provenant d'expéditeurs donnés.

- Reconnaissance floue

  Afin d'échapper au filtrage des spams, les spammeurs ont recours à certaines méthodes visant à entretenir la confusion. Ainsi, certains caractères déterminés, tels que les caractères "*","^", etc., sont insérés de manière arbitraire dans le texte des messages, ou encore des lettres sont remplacées par des caractères similaires, par exemple "porn" pourra être remplacé par "p0rn". Les images peuvent être agrandies ou on peut les faire pivoter. La reconnaissance floue vise à reconnaître ces procédés de contournement et à les filtrer, lorsque cela est autorisé.

- Fréquence d'envoi

  Afin de générer rapidement des spams, les spammeurs peuvent envoyer des messages à un grand nombre de destinataires en peu de temps. Les spammeurs envoient leurs messages beaucoup plus rapidement qu'un expéditeur normal, de sorte que l'intervalle de temps entre deux messages est plus court. Lorsque la fréquence d'envoi de l'utilisateur dépasse le seuil préétabli, l'utilisateur sera identifié comme étant un spammeur hautement suspect.

- Taux d'envoi réussi de messages

  Étant donné que le spam par messagerie est envoyé à des destinataires inconnus, le spammeur choisit les destinataires de manière aléatoire. C'est pourquoi on constate fréquemment que certains numéros appelés sont inexistants. Le taux d'envoi réussi de spams par messagerie est nettement inférieur à celui des messages normaux sur mobile.

- Relevé d'appels de l'expéditeur

  Le relevé d'appels de l'expéditeur peut aider l'opérateur à analyser la configuration de l'envoi. Le relevé devrait comprendre au moins le numéro de téléphone de l'expéditeur, le numéro de téléphone du destinataire et l'heure d'envoi. Si le message est envoyé à un grand nombre d'abonnés et que le taux de réponse est très faible, on peut soupçonner l'expéditeur d'être un spammeur. Les spammeurs utilisent rarement des services fournis par l'opérateur autres que le service de messagerie (appels téléphoniques par exemple).

8.4 Autres améliorations

- Configuration des règles propres à l'utilisateur

  Un mécanisme de configuration des règles propres à l'utilisateur permet aux destinataires de définir le type de message que le destinataire ne souhaite pas recevoir et d'en informer le système de filtrage. Le filtrage des messages selon les règles propres à l'utilisateur peut être effectué par l'opérateur MNO ou au moyen de logiciels installés par les destinataires.

- Réacheminement vers le réseau mobile terrestre public de rattachement (RMTPR) du destinataire

  Les opérateurs peuvent utiliser différents processus antispam pour les clients qui se déplacent hors du réseau RMTPR. Le processus de réacheminement des messages vers le RMTPR étant facultatif, les destinataires en itinérance peuvent recevoir un message sans filtrage des spams. En conséquence, les messages envoyés aux clients en itinérance doivent être réacheminés vers les entités de filtrage antispam du réseau RMTPR, au lieu de s'en remettre au réseau visiteur. Avant d'arriver dans le réseau mobile terrestre public (RMTP) visité, le RMTPR du destinataire doit recevoir et filtrer les messages en prenant les mesures antispam pertinentes.

9 Relations entre les domaines antispam

L'efficacité des mesures antispam dans un domaine antispam unique est limitée, tant du point de vue technique que sur le plan économique. L'interconnexion et l'interfonctionnement sont nécessaires entre les opérateurs MNO et des mécanismes de collaboration entre leurs domaines antispam sont également indispensables. Des mécanismes de collaboration peuvent contribuer à accroître l'efficacité et à améliorer la qualité de fonctionnement des systèmes antispam.

Il existe deux types de relations entre les domaines antispam: une relation de confiance et une relation ne reposant pas sur la confiance (Figure 9-1). La relation par défaut entre domaines antispam devrait être une relation ne reposant pas sur la confiance, auquel cas tous les messages provenant d'homologues non fiables seront filtrés. Dans le cadre d'accords de coopération, la relation de confiance peut être établie entre domaines antispam homologues; pour cette relation, les opérateurs peuvent choisir de ne pas filtrer les messages provenant d'homologues fiables, en fonction de leurs politiques et de leurs règles de filtrage.

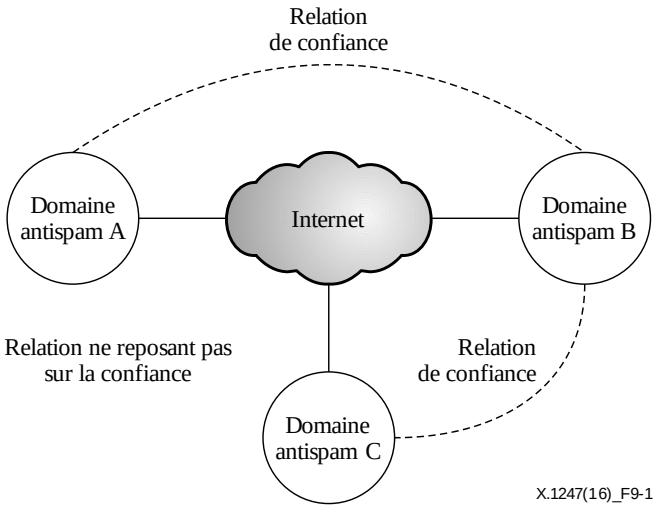

Figure 9-1 – Relation de confiance et relation ne reposant pas sur la confiance

La relation de confiance a un caractère non transitif. Ainsi, si le domaine A fait confiance au domaine B et si le domaine B fait confiance au domaine C, le domaine A ne peut alors pas faire confiance au domaine C, sauf si ces domaines ont négocié et établi directement la relation de confiance. La relation de confiance est bidirectionnelle, ce qui signifie que les homologues de confiance se traitent mutuellement sur un pied d'égalité.

Après l'établissement d'une relation de confiance, il est recommandé d'appliquer les mécanismes de coordination ci-après:

- Échange de données relatives aux spams:

  Certaines données relatives aux spams sont échangées par le biais d'une connexion AMgmt. Les informations ainsi échangées peuvent comporter des listes noires, des mots-clés, des rapports contenant des réclamations et de nouvelles caractéristiques des spams. L'objectif de ces informations sera consulté pendant le processus d'établissement de la relation de confiance. L'échange de données relatives aux spams nécessite l'accord exprès de l'utilisateur final du dispositif mobile et doit être conforme aux réglementations et aux législations nationales.

- Authentification de la source du message

  Le message provenant d'un homologue de confiance ne sera considéré comme authentique que si la source du message est authentifiée.

- Ne pas recourir au filtrage:

  Les messages provenant d'un domaine de confiance peuvent être envoyés directement au destinataire, afin d'éviter tout double emploi dans le traitement du message.

- Rapport contenant une réclamation de l'utilisateur et commentaires sur les spams suspects

  Si des rapports sur des spams et des spams suspects sont reçus sur les messages provenant d'homologues de confiance, il convient de les envoyer aux homologues de confiance, afin d'améliorer leurs règles de filtrage, conformément aux réglementations et législations nationales applicables.

Afin de satisfaire différents mécanismes de coordination, les fonctions APr et AMon devraient mettre en œuvre différentes procédures lorsqu'elles traitent des messages mobiles. La fonction APr décidera si elle filtre ou non le message. En fonction de l'accord, la fonction AMon transmettra/bloquera le message, ou enverra des commentaires aux homologues de confiance. Les Figures 9-2 et 9-3 décrivent les flux opérationnels des fonctions APr et AMon.

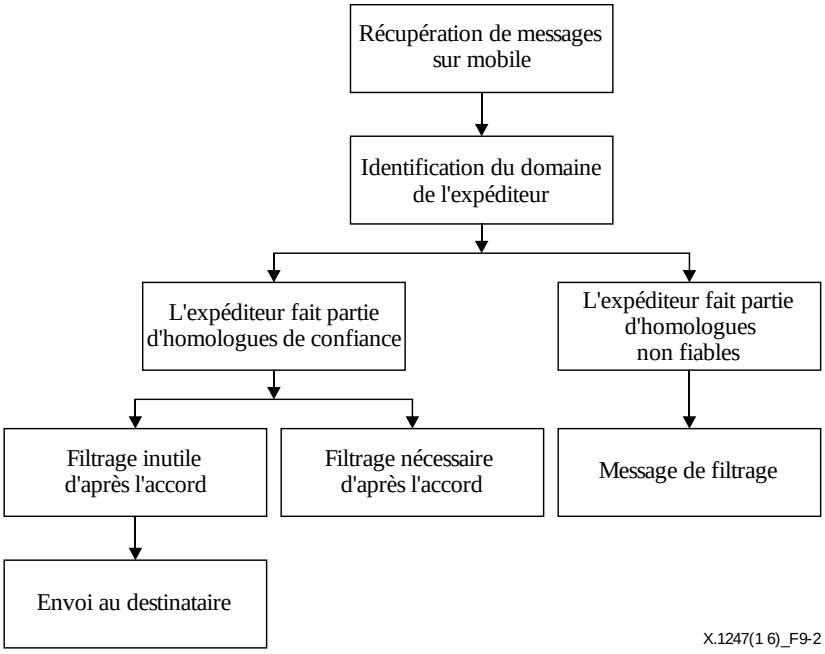

Figure 9-2 – Flux de traitement des messages mobiles dans la fonction APr

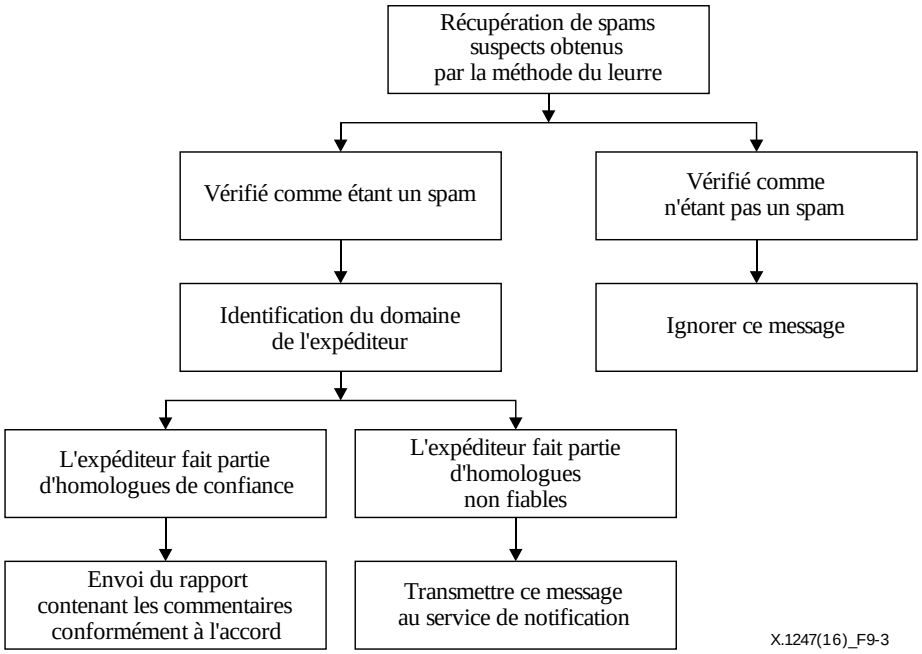

Figure 9-3 – Flux de traitement des messages mobiles dans la fonction AMon

10 Traitement antispam par messagerie mobile

Conformément au processus de traitement antispam par messagerie mobile, il convient de mettre en place un mécanisme adaptatif pour tenir compte de l'apparition constante de nouveaux spams et de leur évolution. En général, on peut considérer que le processus antispam comprend huit procédures, comme indiqué sur la Figure 10-1. Ces procédures constituent un système adaptatif, qui contribue à l'optimisation de la qualité de fonctionnement du système.

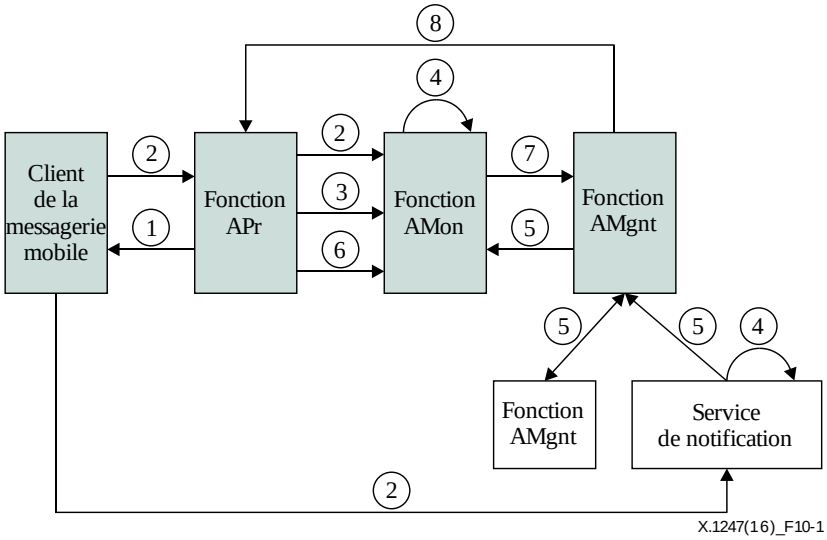

Figure 10-1 – Procédures de traitement antispam

Procédure 1: Filtrage des messages

En fonction des politiques et des règles de filtrage, la fonction APr filtre les messages spam ou leur appose une indication spéciale avant de les envoyer au destinataire. Ces règles de filtrage peuvent être fixées par les opérateurs ou personnalisées par l'utilisateur.

Procédure 2: Envoi de commentaires par l'utilisateur

Le client de la messagerie mobile envoie les réclamations de l'utilisateur au service de notification, afin de signaler le spam non filtré ainsi que les commentaires de l'utilisateur à la fonction AMon, pour indiquer que des messages ont été reçus avec une indication erronée selon laquelle il s'agit d'un spam. Cette procédure aidera les opérateurs à améliorer leurs règles de filtrage.

Procédure 3: Transmission de spams suspects

La fonction APr enverra les spams suspects collectés par le leurre à la fonction AMon pour vérification.

Procédure 4: Vérification du spam

Pour traiter un spam suspect, la fonction AMon vérifie ce spam et informe les services de notification chargés des rapports des utilisateurs sur les spams. Cette procédure est complexe et nécessite une intervention manuelle, conformément aux réglementations et législations nationales applicables. Pour la vérification, il convient d'utiliser des empreintes ou des données hachées sur le spam plutôt que le contenu des messages. Certains renseignements peuvent venir compléter cette appréciation, par exemple la réputation du spammeur et de l'auteur du rapport, et permettront d'évaluer le niveau de confiance du rapport de l'utilisateur.

Procédure 5: Échange d'informations

La fonction AMgmt échange des données relatives aux spams avec les homologues de confiance, et reçoit l'analyse personnalisée des spams émanant du service de notification. Conformément aux résultats de la négociation obtenus par voie de consensus, les données pourront comporter les statistiques figurant dans le rapport de l'utilisateur, la liste des spammeurs, les commentaires figurant dans la réclamation et les nouvelles caractéristiques du spam. Ces données relatives aux spams doivent être traitées avec le plus grand soin, afin de de veiller à ce qu'elles ne comportent aucun contenu de l'utilisateur.

Procédure 6: Contrôle de la qualité de fonctionnement du système

La fonction AMon est également chargée de contrôler la qualité de fonctionnement du système de filtrage des spams. La fonction AMon recueille les données auprès de la fonction APr, afin de créer des rapports sur la qualité de fonctionnement et de les analyser. Le rapport sur la qualité de fonctionnement peut comprendre des chiffres sur la qualité de fonctionnement en temps réel, indiquer le nombre de spams, le taux de faux négatifs, etc.

Procédure 7: Analyse des spams

Les données relatives aux spams confirmés fournies par le service de notification, les homologues de confiance et la fonction AMon seront regroupées et stockées, compte tenu des réglementations et des législations nationales. Périodiquement, la fonction AMon pourra analyser ces données et rechercher de nouvelles configurations et de nouvelles caractéristiques des spams. Cette procédure permettra d'améliorer les règles de filtrage et la qualité de fonctionnement du système. Enfin, elle servira à établir des statistiques sur les spams ainsi qu'un rapport sur l'analyse des spams, qui sera transmis à la fonction AMgmt.

Procédure 8: Ajustement des mesures prises pour lutter contre le spam

En fonction des statistiques sur les spams ainsi que du rapport sur l'analyse des spams communiqués par la fonction AMon, la fonction AMgmt évalue l'efficacité du système de filtrage des spams pour lutter contre le spam, en vue d'éventuelles améliorations. En fonction des résultats de cette évaluation, les mesures et les politiques pourront être adaptées et les mécanismes de collaboration avec d'autres domaines pourront être modifiés. Les mesures correspondantes, par exemple l'établissement ou la suppression de la relation de confiance et l'attribution de nouvelles règles et politiques de filtrage aux fonctions APr, seront alors prises.

Annexe A

Mesures interactives et techniques pour lutter contre les appels non sollicités

(Cette annexe fait partie intégrante de la présente Recommandation.)

Résumé

La présente annexe donne un aperçu des processus visant à enrayer les appels non sollicités et propose une base technique pour lutter contre de tels appels sur la base d'appels vers des numéros (spécialement attribués par l'opérateur télécom) immédiatement après la réception d'un appel non sollicité entrant. Dans ce cadre, il est établi que le ou les opérateurs doivent disposer de numéros anti-spam spéciaux et de fonctions de traitement des enregistrements détaillés des appels à différents niveaux pour ces numéros. De plus, cette Annexe prévoit des mécanismes de partage d'informations pour lutter contre le spam dans le cadre d'interactions inter-opérateurs.

La présente annexe fournit la base technique pour lutter contre le spam lorsqu'un abonné notifie l'opérateur par un bref appel à un numéro anti-spam immédiatement après avoir reçu un appel non sollicité. Cette annexe s'applique au service de téléphonie, au service de messages courts (SMS) et au service de messagerie multimédia (MMS).

Scénario de service de notification interactif pour l'interaction d'un abonné avec un opérateur/fournisseur de services de télécommunications dans le cadre de la lutte contre les appels non sollicités (spams téléphoniques)

La Recommandation UIT-T X.1247 présente le concept de mécanisme de retour d'information des utilisateurs et de rapport d'utilisateur intervenant dans le traitement des messages non sollicités.

La Recommandation [UIT-T X.1246] introduit différents mécanismes de vérification interactive et de traitement anti-spam.

Le mécanisme interactif décrit ici complète et étend les procédures actuelles énoncées dans la Recommandation [UIT-T X.1246] et dans la partie principale de la présente Recommandation (UIT-T X.1247). L'interaction proposée d'un abonné/destinataire d'un appel non sollicité avec un opérateur/fournisseur de services de télécommunications consiste pour l'abonné à passer un bref appel vers un numéro anti-spam spécifique d'un tel opérateur/fournisseur de services de télécommunications ou à transférer le message non sollicité reçu vers ce numéro.

A.1 Scénario/algorithme/cas d'utilisation pour le retour d'information interactif

Le scénario qui consiste à appeler un numéro anti-spam pour déterminer un appel non sollicité à l'aide du traitement automatique des détails d'un CDR/CLI comprend les étapes suivantes:

1) Le destinataire/client/abonné reçoit un appel entrant qu'il identifie/définit comme un appel non sollicité ou appel non sollicité suspect (spam vocal, SMS ou MMS).

2) Les données CDR/CLI relatives à cet appel (ainsi qu'à tout autre appel) sont sauvegardées dans le système de gestion des télécommunications (ou dans un autre ou plusieurs systèmes) de l'opérateur de télécommunications. Ces données contiennent l'identifiant de l'appelant (source possible de l'appel non sollicité), l'identifiant du destinataire de l'appel (destinataire de l'appel non sollicité) et l'heure de l'appel.

3) Immédiatement/le plus rapidement possible après avoir terminé cet appel, le destinataire/client/abonné compose un numéro spécial anti-spam défini à l'avance par son opérateur/fournisseur de services de télécommunications propre/national (selon la réglementation du pays, un tel numéro peut être unique à l'échelle nationale ou spécifique à chaque opérateur), autrement dit, il passe un appel sortant vers un numéro anti-spam sous la forme d'un rapport d'utilisateur interactif.

4) Les données CDR_{n+1}/CLI_{n+1} relatives à cet appel sont également sauvegardées dans le système de gestion des télécommunications de l'opérateur.

5) L'opérateur, qui reçoit un appel de ce type sur le numéro anti-spam de l'abonné, saisit toutes les données techniques CDR_{n+1} (CDR et CLI avec différents niveaux de détail), retrouve automatiquement l'avant dernier appel CDR_n entrant passé à l'abonné/au destinataire d'un éventuel appel non sollicité et commence à collecter des informations sur un possible appel non sollicité (en échangeant éventuellement ces informations avec d'autres opérateurs/régulateurs).

6) Si l'appel passé sur le numéro anti-spam s'avère isolé et/ou erroné, aucune autre démarche ne sera requise.

7) S'il y a plusieurs appels vers le numéro anti-spam en provenance de plusieurs destinataires de possibles appels non sollicités, et si dans chaque cas le système de traitement CDR identifie le même numéro d'appelant ou CLI_n du dernier appel entrant vers l'abonné/utilisateur avant son appel sortant au numéro anti-spam, la probabilité de détecter la véritable source des appels non sollicités pour trouver le spammeur sera plus grande.

8) Il est possible de définir en option différents seuils pour les systèmes de traitement CDR afin d'éliminer les fausses alarmes.

A.2 Spécifications techniques

A.2.1 S'il souhaite recevoir des appels de retour d'information en provenance des destinataires, l'opérateur/le fournisseur de services de télécommunications devra disposer d'un numéro anti-spam spécial.

A.2.2 Pour pouvoir traiter un nombre important d'appels de retour d'information, le système de gestion des télécommunications de l'opérateur/du fournisseur de services de télécommunications doit avoir la possibilité de recevoir et de traiter ces appels exclusivement sur la base des relevés CDR et données CLI de niveau inférieur.

A.2.3 Le système de gestion des télécommunications doit garantir une qualité de service des données statistiques du service de notification.

Bibliographie

[b-UIT-T X.1240] Recommandation UIT-T X.1240 (2008), *Technologies intervenant dans la lutte contre le spam par courrier électronique.*

[b-UIT-T X.1242] Recommandation UIT-T X.1242 (2009), *Système de filtrage du spam du service de messages courts (SMS) fondé sur les règles définies par l'utilisateur.*

[b-M3AWG report] Rapport M3AAWG, *Mobile Messaging Best Practices for Service Providers*, mis à jour en août 2015.
https://www.m3aawg.org/sites/default/files/M3AAWG-Mobile-Messaging-Best-Practices-Service-Providers-2015-08.pdf

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
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	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; 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	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements 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, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2022