Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1246

Amendement 1

(05/2022)

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

Sécurité du cyberespace – Lutte contre le spam

Technologies intervenant dans la lutte contre le spam vocal dans les organisations de télécommunication

Amendement 1

Recommandation UIT-T X.1246 (2015) – 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.1246

Technologies intervenant dans la lutte contre le spam vocal dans les organisations de télécommunication

Amendement 1

Résumé

Les communications vocales constituent un service fondamental fourni sur les réseaux de télécommunication. Avec l'essor des communications vocales, le nombre de spams vocaux a augmenté et a eu de nombreuses conséquences négatives pour les utilisateurs finals et les opérateurs de réseau. En général, les spams vocaux peuvent comprendre aussi bien des publicités commerciales que des contenus inappropriés à caractère pornographique, qui ont des retombées négatives diverses sur les utilisateurs finals et les opérateurs de réseau. Les spams vocaux peuvent avoir pour effet d'attirer, d'importuner, de harceler, voire d'intimider les utilisateurs et avoir des conséquences négatives sur les ressources de réseau. Pour éviter ces incidences négatives et protéger les droits des utilisateurs tout en maintenant la stabilité des réseaux, les opérateurs de réseau voudront peut-être intensifier leurs efforts dans la lutte contre le spam vocal.

L'objectif de la Recommandation UIT-T X.1246 est de passer en revue les solutions techniques de lutte contre le spam vocal, sans tenir compte du risque quant à l'authenticité de l'identité du spammeur. La présente Recommandation donne un aperçu du spam vocal, expose les technologies anti-spam actuellement utilisées par les utilisateurs ainsi que les réseaux de télécommunication et décrit les mécanismes de collaboration entre elles. D'autres solutions techniques proposées sont également recommandées sur la base de ces technologies anti-spam et de ces mécanismes de collaboration.

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

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1246	17-09-2015	17	11.1002/1000/12448
1.1	UIT-T X.1246 (2015) Amd. 1	20-05-2015	17	11.1002/1000/14988

Mots clés

Spam, spam vocal.

* 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 on 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

Recommandation UIT-T X.1246

Technologies intervenant dans la lutte contre le spam vocal dans les organisations de télécommunication

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.1246 (2015).

1 Domaine d'application

La présente Recommandation donne un aperçu du spam vocal et passe en revue les technologies actuellement utilisées pour faciliter la lutte contre le spam vocal, y compris les technologies côté réseau et celles côté utilisateur ainsi que le mécanisme de collaboration entre elles. En outre, elle propose d'autres solutions pratiques pour lutter contre le spam (relevés de signalisation, vérification interactive, mesures de contrôle, etc.).

La présente Recommandation porte uniquement sur la lutte contre le spam vocal ayant pour origine la partie à commutation de circuits des réseaux de télécommunication, compte tenu des caractéristiques particulières de l'infrastructure de réseau. En ce qui concerne les technologies de lutte contre le spam vocal ayant pour origine la partie IP, on se reportera aux Recommandations [UIT-T X.1244] et [b-UIT-T X.1245] et à la norme [b-IETF RFC 5039]. Les technologies qui permettent d'éviter l'usurpation de l'identité de l'appelant n'entrent pas dans le cadre de la présente Recommandation.

Il convient de tenir compte de toutes les législations et réglementations pertinentes, avant d'adopter les méthodes antispam décrites dans la présente Recommandation.

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.

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

[UIT-T X.1244] Recommandation UIT-T X.1244 (2008), *Aspects généraux de la lutte contre le spam dans les applications multimédias IP*.

[UIT-T X.1247] Recommandation UIT-T X.1247 (2016), *Cadre technique de lutte contre le spam par messagerie mobile*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 réseau à commutation de circuits [b-ITU-T M.60]: réseau qui fournit des connexions à l'usage exclusif des utilisateurs pour la durée d'une communication ou d'un service, en interconnectant des canaux de transmission ou des circuits de télécommunication.

3.1.2 réseau IP [b-ITU-T E.370]: réseau dans lequel le protocole Internet est utilisé en tant que protocole de la couche 3 de l'ISO (modèle de référence OSI).

3.1.3 opérateur [b-ITU-T M.1400]: organisme chargé d'identifier et de gérer des ressources de télécommunication. L'opérateur doit être reconnu juridiquement par l'administration des télécommunications du pays en question, ou par la délégation de ce dernier. Un opérateur peut représenter un partenaire commercial.

~~**3.1.4 spammeur** [b-ITU-T X.1231]: entité ou personne qui crée et envoie des spams.~~

3.1.4 service de notification [UIT-T X.1247]: 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.

3.1.5 service de messages courts (SMS, *short message service*) [b-UIT-T X.1231]: 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.

3.1.6 spam par SMS [b-UIT-T X.1242]: spam envoyé par SMS.

3.1.7 spam [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.

3.1.8 spammeur [UIT-T X.1240]: entité ou personne qui crée et envoie des spams.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 numéro anti-spam: 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.

3.2.2 leurre (*honeypot*): progiciel (éventuellement dans un terminal) qui émule un terminal ou un groupe de terminaux afin de détecter les spammeurs téléphoniques présumés et de contribuer à faire des vérifications. Les résultats obtenus par ce type de système peuvent servir à rassembler des preuves.

3.2.3 rapport d'utilisateur interactif: 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.

3.2.~~3~~4 entité de gestion: entité chargée de diriger, de vérifier ou de guider les activités de lutte contre le spam vocal.

3.2.5 appel non sollicité: appel téléphonique contenant un message vocal, texte ou multimédia non sollicité et visant généralement à faire de la publicité de produits ou services commerciaux.

3.2.6 appel non sollicité suspect: appel téléphonique indéterminé soupçonné d'être un spam.

3.2.~~4~~7 organisme tiers: entité qui peut consulter, faciliter ou coordonner les activités de lutte contre le spam vocal.

3.2.~~1~~8 spam vocal: appel téléphonique non sollicité, pré-enregistré, dont le numéro est composé automatiquement, dont l'objectif est généralement de faire de la publicité de produits ou services commerciaux. Un spam vocal peut comprendre aussi bien une publicité commerciale que des contenus inappropriés à caractère pornographique, qui ont diverses conséquences négatives pour les utilisateurs et les opérateurs.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

Caller ID identification de l'appelant (*caller identification*)

CAMEL applications spécialisées de logique mobile améliorée (*customized applications for obile enhanced logic*)

CCLTP instant de libération de l'appel (*call clear time point*)

CCOTP instant de mise en relation (*call continued time point*)

CDMA accès multiple par répartition en code (*code division multiple access*)

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 feedback call to an anti-spam number*)

COSN numéro d'abonné d'origine de l'appel (*call originated subscriber number*)

COTP instant de lancement de l'appel (*call originating time point*)

CRBT tonalité de retour d'appel personnalisée (*colour ring back tone*)

CS commutation de circuits (*circuit-switched*)

CTSN numéro d'abonné de destination de l'appel (*call terminated subscriber number*)

DMP plate-forme de gestion des dispositifs (*device management platform*)

GMSC centre de commutation passerelle pour les services mobiles (*gateway mobile switching centre*)

GSM système mondial de communications mobiles (*global system for mobile communications*)

HLR registre de localisation dans le réseau de rattachement (*home location register*)

ID identification

IMS sous-système multimédia IP (*IP multimedia subsystem*)

IN réseau intelligent (*intelligent network*)

INAP protocole d'application de réseau intelligent (*intelligent network application protocol*)

IP protocole Internet (*Internet protocol*)

ISIS système de partage d'informations (*information sharing system*)

IVR réponse vocale interactive (*interactive voice response*)

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

MSC centre de commutation pour les services mobiles (*mobile switching centre*)

OTAP plate-forme hertzienne (*over-the-air platform*)

QoS qualité de service (*quality of service*)

RTPC réseau téléphonique public commuté

SCP point de commande de service (*service control point*)

SIM module d'identité d'abonné (*subscriber identity module*)

SLETP instant d'établissement de la liaison de signalisation (*signalling link establishment time point*)

SLRTP instant de libération de la liaison de signalisation (*signalling link release time point*)

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

SS7 système de signalisation N° 7 (*signalling system no.7*)

STP point de transfert de signalisation (*signalling transfer point*)

UMTS système de télécommunications mobiles universelles (*universal mobile telecommunications system*)

VLR registre de localisation des visiteurs (*visitor location register*)

VMS serveur de messagerie vocale (*voice mail server*)

VoIP téléphonie utilisant le protocole Internet (*voice over internet protocol*)

5 Conventions

Aucune.

6 Aperçu du spam vocal

Un spam vocal est un appel téléphonique non sollicité, pré-enregistré, dont le numéro est composé automatiquement, qui vise généralement à faire de la publicité de produits ou services commerciaux. Un spam vocal peut comprendre aussi bien une publicité commerciale que des contenus inappropriés à caractère pornographique, qui ont diverses conséquences négatives pour les utilisateurs et les opérateurs.

6.1 Scénarios de communication vocale

Les communications vocales constituent un service fondamental fourni par les opérateurs de télécommunication. Au départ, ces communications étaient assurées sur les réseaux traditionnels à commutation de circuits (CS). Avec l'essor de l'Internet, les communications vocales englobent désormais aussi les communications VoIP sur les réseaux IP.

Quatre scénarios de communication vocale, chacun déterminé par les technologies utilisées, sont examinés ci-après:

- Scénario 1: CS-CS: Communication vocale sur un réseau mobile/fixe à commutation de circuits traditionnel.
- Scénario 2: CS-IP: Communication vocale ayant pour origine un utilisateur de réseau mobile/fixe à commutation de circuits et pour destination un utilisateur de téléphonie IP.
- Scénario 3: IP-CS: Communication vocale ayant pour origine un utilisateur de téléphonie IP et pour destination un utilisateur de réseau mobile/fixe à commutation de circuits.
- Scénario 4: IP-IP: Communication vocale entre utilisateurs de téléphonie IP.

Ces quatre scénarios de communication et les technologies connexes sont représentés sur la Figure 1.

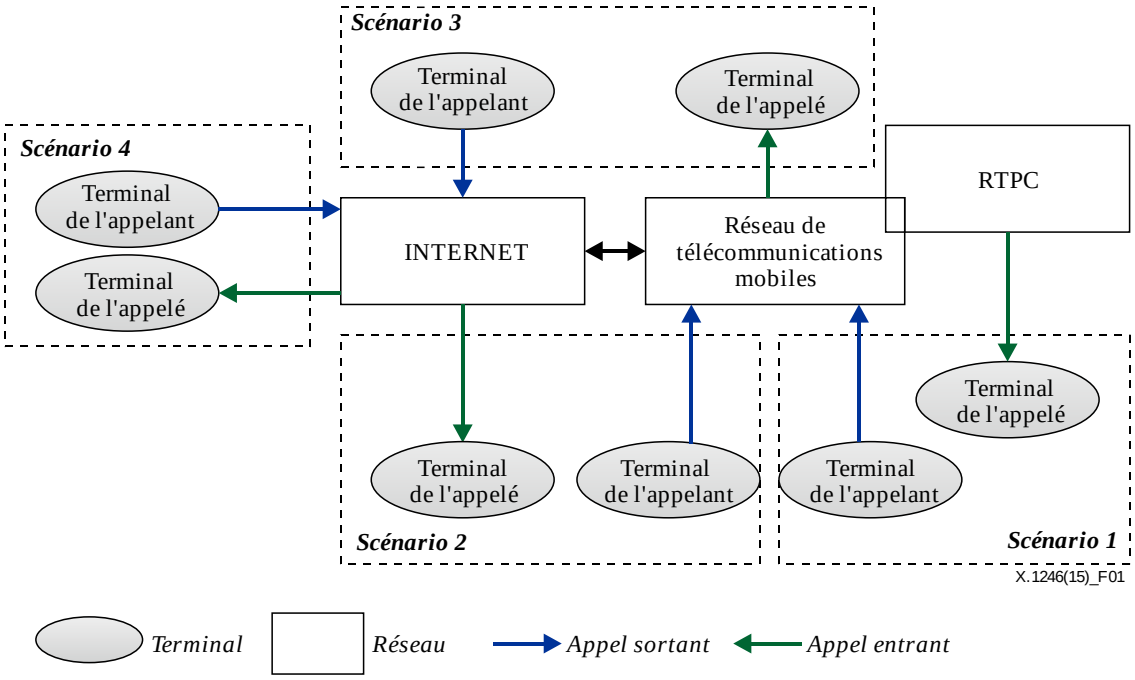

Figure 1 – Scénarios de communications vocales sur les réseaux de télécommunication

NOTE – Le mot "terminal", au sens où il est employé dans la Figure 1, peut désigner des téléphones mobiles, des téléphones fixes, des ordinateurs portables, des ordinateurs personnels, etc., qui permettent d'accéder à des réseaux à commutation de circuits/IP. D'une manière générale, la plupart des utilisateurs font confiance à l'origine des télécommunications vocales, ce qui incite les spammeurs téléphoniques à lancer des spams vocaux sur les réseaux traditionnels à commutation de circuits. De plus, étant donné que des technologies de lutte contre le spam vocal dans les scénarios 3 et 4 sont recommandées dans la Recommandation [ITU-T X.1244], la présente Recommandation ne porte que sur la lutte contre le spam vocal dans le scénario 1 (CS-CS) et dans le scénario 2 (CS-IP).

6.2 Caractéristiques du spam vocal

Un spam vocal peut diffuser aussi bien une publicité commerciale que du contenu inapproprié à caractère pornographique, qui peuvent avoir des conséquences négatives pour les utilisateurs et les opérateurs de réseau:

– Un spam vocal peut comporter un contenu fastidieux, fallacieux, intimidant ou menaçant.

– Les utilisateurs et les opérateurs peuvent subir un gaspillage de ressources.

– La lutte contre le spam vocal peut demander du temps, de l'argent et des efforts aux utilisateurs et aux opérateurs.

Parmi les formes les plus répandues de spam vocal, on peut distinguer deux types, sans que cette liste soit exhaustive:

– **Premier type (appel silencieux)**: un appel silencieux est un appel téléphonique à visée publicitaire, qui est généré par un ou plusieurs composeurs automatiques prédictifs sans qu'il soit prévu qu'un agent traite immédiatement l'appel. En pareil cas, il peut être mis fin à l'appel par le composeur automatique, et l'appelé reçoit un silence ("temps mort") ou une tonalité de la part de l'entreprise téléphonique qui indique que l'appel a été abandonné. Le terme "appel abandonné" a la même signification. En général, avec ce type d'appel, un rappel est attendu.

– **Deuxième type (appel de harcèlement)**: appel téléphonique à visée publicitaire, qui peut aussi avoir pour conséquence de harceler, d'importuner, d'alarmer ou d'intimider en raison d'un contenu pornographique, d'une menace, d'informations illégales, d'une fausse publicité, etc. En général, ce type d'appel ne sera pas abandonné avant la mise en relation.

7 Technologies de lutte contre le spam vocal

7.1 Aspects généraux

Utilisée de manière indépendante, aucune des solutions ne sera entièrement satisfaisante. Pour atténuer les 'incidences négatives du spam vocal, il est nécessaire de mettre en place un ensemble complet de solutions avec des technologies corrélées, qui sont classées dans deux catégories, à savoir les technologies côté réseau et les technologies côté utilisateur, pour tenir compte des scénarios 1 et 2 décrits au § 6.1.

Pour recommander des technologies concrètes et pratiques, il est nécessaire d'examiner de manière approfondie les caractéristiques du réseau à commutation de circuits, y compris l'architecture et la topologie du réseau, la pile de protocoles de signalisation, etc. En outre, il convient d'examiner les processus du service vocal et l'évolution fonctionnelle des terminaux. Les technologies recommandées peuvent être classées en technologies côté réseau et technologies côté utilisateur.

Les technologies côté réseau, autrement dit celles qui sont mises en œuvre dans les réseaux téléphoniques publics commutés (RTPC), dans les systèmes de télécommunications mobiles universelles (UMTS), dans le système mondial de communications mobiles (GSM) et dans les réseaux à accès multiple par répartition en code (CDMA), sont essentielles pour les opérateurs. Par rapport aux technologies côté réseau, les technologies côté utilisateur sont beaucoup plus souples et sont mises en œuvre à l'initiative de l'utilisateur. Les commentaires des utilisateurs constituent un complément indispensable aux technologies côté réseau. Il convient donc d'établir aussi un mécanisme de collaboration efficace entre les deux types de technologies.

7.2 Technologies côté réseau

Chaque appel téléphonique est lancé dans le réseau d'accès au moyen d'une procédure de signalisation. Pour détecter un spammeur téléphonique présumé, la méthode de base consiste à recueillir les données de signalisation, à les analyser et à les vérifier. Cette méthode devrait être examinée sous tous les angles. D'une manière générale, la phase d'établissement d'un appel fait intervenir une prise de contact entre les deux extrémités de la communication. Pendant cette phase, la seule identification de l'appelant/appelé est celle de l'appelant, ce qui conduit à l'observation suivante.

1) Toute décision relative au traitement de l'appel devrait être prise en temps réel avant la fin de l'établissement de l'appel.

Le spam vocal pose des problèmes techniques complexes, de sorte que les solutions mises en œuvre pour en venir à bout doivent s'appuyer sur des procédures appropriées, associées à des mesures techniques. Une procédure de base côté réseau à appliquer pour lutter contre le spam vocal pourrait comprendre les processus suivants indiqués dans la Figure 2:

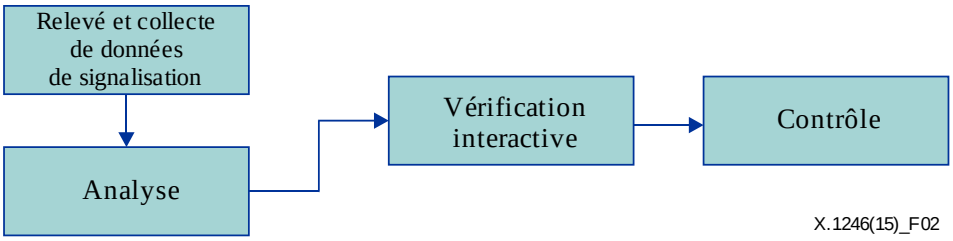

Figure 2 – Procédure côté réseau pour lutter contre le spam vocal

– **Relevé et collecte de données de signalisation**: Relever et recueillir des données de signalisation d'origine en temps réel.

– **Analyse**: Identifier les spammeurs téléphoniques présumés et dresser la liste de leurs numéros.

– **Vérification interactive**: Procéder à une vérification directe pour repérer les vrais spammeurs téléphoniques dans la liste des numéros suspects.

– **Contrôle**: Limiter ou interdire les appels provenant des spammeurs téléphoniques confirmés comme tels par le processus de vérification afin de protéger les utilisateurs normaux.

La procédure côté utilisateur fait intervenir à peu près les mêmes processus, mais avec des mesures plus simples. Dans certains cas, la vérification interactive peut être omise.

Conformément à la procédure, plusieurs technologies peuvent être employées pour chacun des processus. Il est à noter qu'aucune des technologies examinées dans les paragraphes qui suivent ne constituera un remède miracle ou la seule et unique solution aux problèmes posés par le spam vocal. Toutes les technologies sont complémentaires et leur efficacité sera renforcée si elles sont employées ensemble.

Dans la présente Recommandation, les technologies sont présentées et classées en fonction de l'emplacement où elles sont déployées, à savoir côté réseau ou côté utilisateur, et en fonction des processus (indiqués dans la Figure 2).

7.2.1 Relevé et collecte de données de signalisation

Le relevé et la collecte de données de signalisation consistent à recueillir en temps(quasi) réel, en vue de leur analyse, des données de relevé détaillé des appels, qui peuvent comprendre des données temporelles ou des données relatives au numéro de téléphone, par exemple:

– instant d'origine de l'appel (COTP): instant auquel un appelant lance un appel téléphonique;

– instant d'établissement de la liaison de signalisation (SLETP): instant auquel la liaison de signalisation est établie entre un appelant et un appelé;

– instant de mise en relation (CCOTP): instant auquel l'appelé donne suite à l'appel et la mise en relation est assurée;

– instant de libération de l'appel (CCLTP): instant auquel l'appel est libéré par un appelant ou un appelé;

– instant de libération de la liaison de signalisation (SLRTP): instant auquel la liaison de signalisation est libérée après la libération d'un appel;

– numéro d'abonné d'origine de l'appel (COSN): généralement appelé numéro de l'appelant, il s'agit du numéro d'un appel auquel met fin un appelant;

– numéro d'abonné de destination de l'appel (CTSN): généralement appelé numéro de l'appelé, il s'agit du numéro auquel l'appel est destiné.

Les valeurs des mêmes données, en particulier des données temporelles, peuvent varier légèrement en fonction de la position des points de collecte. Toutefois, ces disparités peuvent toujours être omises dans la pratique.

Il est à noter que toutes les données visées dans le présent paragraphe proviennent des canaux de signalisation, et non des canaux de service. Dans ce processus de relevé des données de signalisation, toutes les données à collecter existent généralement dans le système de gestion de la signalisation à des fins de comptabilité et de diagnostic de la qualité de fonctionnement, et peuvent donc être réutilisées dans un souci de maîtrise des coûts.

NOTE – Seules les sources de données courantes (fondées sur le système de signalisation N° 7 (SS7), le réseau intelligent, le sous-système multimédia IP (IMS), le service de tonalité de retour d'appel personnalisée (CRBT), le serveur de messagerie vocale (VMS), etc.) seront citées ci-dessous, mais il existe d'autres sources de données possibles, comme le système R2 et les systèmes d'alerte en cas d'appel manqué.

7.2.1.1 Système de signalisation N°7 (SS7)

Le système de signalisation N° 7 peut être utile pour faciliter le contrôle du spam vocal. Il est commode d'insérer un point de collecte des données de signalisation pour dupliquer les informations et les paramètres de signalisation, et les enregistrer. Ce point de collecte est connecté en parallèle avec la liaison de signalisation, de sorte que le signal est scindé, mais seule une petite partie de la puissance du signal sera consommée par le point de collecte. En pareil cas, une défaillance du point de collecte ne doit avoir aucune incidence négative sur la liaison de signalisation.

Il existe une autre méthode pour collecter les données de signalisation SS7, dans laquelle un nœud de signalisation caché est inséré entre deux nœuds de signalisation explicites. Ce nœud caché va d'abord "bloquer" le signal pour l'enregistrer, puis le relayer sans modification, mais avec une certaine latence. Toutefois, cette technologie présente un risque de point de défaillance isolé. Il faut donc prévoir une capacité fiable de secours en cas de défaillance.

L'utilisation des relevés de signalisation SS7 est particulièrement intéressante, en ce sens que les relevés contiennent les données détaillées des appels à partir desquelles on peut obtenir divers indicateurs (voir le § 7.2.2). Toutefois, si le trafic des appels vocaux augmente et que le réseau se développe, le nombre de points de collecte des données de signalisation devra augmenter en conséquence pour tenir compte des principales/de toutes les sources de signalisation, afin d'assurer un contrôle acceptable, ce qui entraînera peut-être des coûts plus élevés pour la lutte contre le spam.

Il est recommandé de déployer les points de collecte des données de signalisation dans les réseaux centraux/locaux. Pour assurer une collecte globale, ces points doivent couvrir toutes les interfaces Mc et Nc des commutateurs, tandis que pour assurer une collecte équilibrée, ces points doivent couvrir uniquement toutes les interfaces Nc. Si l'on s'intéresse uniquement aux appels nationaux longue distance ou aux appels internationaux, les points de transfert sémaphores (STP) longue distance/internationaux doivent être traités.

NOTE – Le point de collecte des données de signalisation est un élément de réseau logique, qui peut prendre la forme de différents types d'éléments d'entité.

7.2.1.2 Réseau intelligent (IN)

Une méthode fondée sur les points de commande de service (SCP) consiste à recueillir les applications spécialisées pour la logique mobile améliorée (CAMEL) ou le protocole d'application de réseau intelligent (INAP) à des fins d'analyse. Le point SCP est un nœud essentiel dans les réseaux intelligents et un facteur déterminant pour décider de la manière de traiter les appels téléphoniques.

Une fois qu'un utilisateur a souscrit à un service de réseau intelligent, pour tout appel sortant, le point SCP demandera des renseignements sur le registre de localisation des visiteurs (VLR) de l'usager appelé avant d'établir des liaisons de communication. Etant donné que les services de réseau intelligent sont couramment utilisés par certains opérateurs, on peut aisément collecter et enregistrer les données de signalisation des appels lancés par les utilisateurs ayant souscrit à un service de réseau intelligent.

Étant donné que les points de collecte des données de signalisation peuvent se trouver au niveau ou au voisinage de points SCP, la méthode nécessite moins de points de collecte de données de signalisation que celle du système SS7. Que les utilisateurs ayant souscrit à un service de réseau intelligent soient en itinérance ou non, cette méthode permet de les contrôler sans difficulté.

Toutefois, cette méthode présente un inconvénient. Si le taux de pénétration des services de réseau intelligent reste faible, seule une petite partie des comportements des utilisateurs sera contrôlée. Néanmoins, on peut remédier à cette situation en aidant chaque utilisateur à souscrire implicitement à un service personnalisé de réseau intelligent, qui transmettra la demande d'informations sans condition au point SCP lorsqu'un appel sortant est établi.

Un autre inconvénient de cette méthode est que le processus général de service de réseau intelligent ne permet de collecter que des types de données limités, par exemple COTP, SLETP, COSN et CTSN (voir le § 7.2.1). Néanmoins, des améliorations sont possibles si un processus plus complexe de service de réseau intelligent est mis en place, par exemple si tous les signaux de signalisation téléphonique sont retransmis par des points SCP.

La méthode relative au sous-système multimédia IP (IMS) est analogue à celle décrite ci-dessus, étant donné que le sous-système IMS utilise des procédures de signalisation analogues à celles utilisées par le réseau intelligent.

7.2.1.3 Tonalité de retour d'appel personnalisée (CRBT)

Le service CRBT est un service spécialement orienté vers l'utilisateur qui est fourni par certains opérateurs. Une fois qu'un utilisateur a souscrit au service CRBT, les autres utilisateurs entendront des séquences musicales précommandées au lieu de la tonalité de retour d'appel. En conséquence, les données de signalisation peuvent être recueillies et enregistrées dans les serveurs CRBT.

Cette méthode présente un inconvénient. En effet, le processus du service ne permet de collecter que des types de données limités dans les serveurs du service, par exemple COTP, CCOTP, CCLTP, COSN et CTSN (voir le § 7.2.1). Pratiquement aucune autre amélioration ne peut être apportée au processus CRBT pour collecter d'autres types de données.

Cependant, si un spammeur téléphonique importune un utilisateur CRBT, le spammeur pourra être surveillé. En conséquence, une forte pénétration du service est une condition indispensable pour que cette méthode soit utilisable. Si cette condition est remplie, les investissements liés à l'enregistrement et à la collecte des données de signalisation devraient être relativement faibles.

7.2.1.4 Serveur de messagerie vocale (VMS)

Les serveurs de messagerie vocale (VMS) traitent les appels dans les cas suivants: renvoi d'appel sur non-réponse, renvoi d'appel sur occupation, renvoi d'appel inconditionnel, etc. Le plus souvent, le serveur VMS ne réagit pas à un appel silencieux, sauf dans le cas "inconditionnel". Le serveur VMS peut fournir des enregistrements vocaux d'un appelant si le spammeur cherche à faire établir l'appel et à envoyer directement un spam à l'appelé. En pareil cas, le serveur VMS pourra appuyer sans réserve le processus de vérification interactive par l'intermédiaire des enregistrements vocaux provenant des commentaires formulés par l'utilisateur ou de l'autorisation (voir le § 7.3.3).

Comme pour le service CRBT, le taux de pénétration du service et l'utilisation du serveur VMS sont des conditions indispensables pour que cette méthode soit utilisable.

7.2.1.5 Leurre

La méthode du leurre est utilisée pour mettre en place un certain nombre de numéros de téléphone successifs ou aléatoires en vue d'attirer les spammeurs téléphoniques. Hormis la collecte de données, cette méthode peut aussi faciliter la procédure d'analyse ainsi que la procédure de vérification interactive.

Etant donné que la méthode du leurre peut être menée à bien par n'importe quel appelant (appel sortant), elle permet de collecter certains types particuliers de données, par exemple COTP, CCOTP, CCLTP, COSN et CTSN (voir le § 7.2.1). La méthode du leurre permettra de calculer et de transférer les données en vue de réaliser certaines des mesures analytiques décrites au § 7.2.2.

7.2.2 Analyse

Pour pouvoir effectuer une analyse de la lutte contre le spam vocal au moyen du système de surveillance, les données d'origine recueillies doivent être calculées et transformées en indicateurs significatifs, par exemple le taux de connexion, l'instant de libération de l'appel, la durée de la tonalité, etc. Afin de différencier les spammeurs téléphoniques des utilisateurs normaux, les indicateurs doivent faire l'objet d'un comptage en continu pendant une période donnée, généralement appelée fenêtre temporelle (durée). Les opérateurs peuvent régler la durée sur une valeur appropriée en fonction de l'expérience acquise.

A partir de tous les indicateurs, on peut déduire logiquement un indicateur plus détaillé appelé "la règle", qui peut être utilisé dans certains algorithmes pour analyser le comportement du spammeur téléphonique avec une plus grande précision. Le modèle de règle à utiliser pour analyser le spammeur téléphonique est représenté sur la Figure 3.

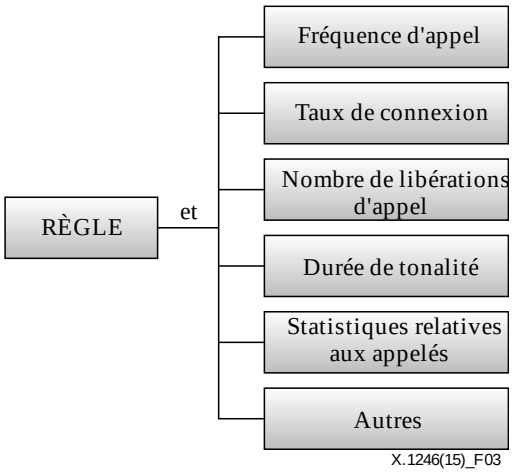

Figure 3 – Modèle de règle

Le modèle de règle est déduit de plusieurs indicateurs par l'opération logique ET. Etant donné que les données proviennent de sources différentes et peuvent être recueillies ensemble, les indicateurs ne peuvent pas tous être pris en charge en même temps. Pour résoudre le problème, une solution possible consiste à mettre les indicateurs non pris en charge à "VRAI" ou à "1" pour les ignorer. Par exemple, après avoir collecté les données et les avoir transformées en indicateurs, le leurre a uniquement besoin que l'indicateur de durée de tonalité exécute la procédure d'analyse requise et mette la valeur des autres indicateurs à "VRAI" ou "1" pour les omettre.

Les indicateurs figurant dans le modèle de règle et leurs définitions sont énumérés ci-après:

– fréquence d'appel: nombre d'appels pendant une période donnée;

– taux de connexion: taux d'établissement de la communication ou de la liaison de signalisation;

– nombre de libérations d'appel: nombre de fois où l'appelant ou l'appelé libère l'appel de sa propre initiative;
– durée de tonalité: durée de la sonnerie;
– statistiques relatives aux appelés: statistiques sur les caractéristiques des appelés, par exemple répartition uniforme, progression arithmétique, etc.

La valeur seuil des indicateurs devrait être ajustée par les opérateurs sur la base de scénarios de service réalistes pour parvenir à un compromis entre la précision et le coût. En outre, il convient de définir les règles concrètes pour tenir compte des différents types de spam vocal.

Par exemple, il existe deux types de spam vocal bien connus: les appels silencieux et les appels de harcèlement (voir le § 6.2). Un appel silencieux (également appelé appel abandonné) est un appel téléphonique lancé par un composeur automatique sans qu'un agent soit disponible immédiatement pour traiter l'appel. En pareil cas, le composeur automatique peut mettre fin à l'appel et l'appelé reçoit un silence ("temps mort") ou une tonalité de la part de l'entreprise téléphonique, qui indique que l'appel a été abandonné. En général, avec ce type d'appel, un rappel est attendu. Un appel de harcèlement est un appel téléphonique destiné à harceler, importuner, alarmer ou intimider avec un contenu à caractère pornographique, des menaces, des informations illégales et de fausses publicités, etc. En général, ces appels ne seront pas abandonnés avant la mise en relation.

Les appels silencieux et les appels de harcèlement (voir le § 6.2) présentent parfois des caractéristiques différentes pour les indicateurs dans le cadre du modèle de règle proposé. Une valeur élevée pour la fréquence d'appel ou le nombre de libérations d'appel et une valeur faible pour le taux de connexion ou la durée de sonnerie peuvent faire penser à un spammeur qui envoie des appels silencieux. En revanche, les appels de harcèlement sont parfois ciblés sur un appelé particulier et, comparativement, la sonnerie a tendance à être maintenue plus longtemps et le taux de connexion à être plus élevé.

Dans certains cas, un groupe de spammeurs envoyant des appels silencieux va ouvrir le service de "renvoi inconditionnel" pour indiquer au réseau qu'il doit renvoyer les appels entrants sans condition vers un numéro donné, sur lequel fonctionne une plate-forme de réponse vocale interactive (IVR). La plate-forme IVR peut même retourner le spam vocal à l'appelant au moyen d'une sonnerie. Il serait utile, pour l'analyse, de vérifier si les appelants présumés ont ouvert le service de "renvoi inconditionnel" et quel était le numéro de destination.

Il existe certes d'autres modèles d'analyse plus complexes et efficaces pour lutter contre le spam vocal, par exemple un modèle intégré à une analyse de la société humaine, une analyse des relevés des appels facturés aux appelants, etc. Cependant, le modèle de règle pourrait servir de base à l'élaboration de modèles plus complets.

7.2.3 Vérification interactive

Comme l'exigent les entités de gestion ou l'accord de service de l'utilisateur, le numéro de l'appelant figurant sur la liste des numéros suspects doit être vérifié avant que des mesures de contrôle ne soient prises. Il existe deux méthodes possibles pour procéder à la vérification requise.

Selon la première méthode, les organisations de télécommunication doivent tenir à jour la liste des numéros suspects, la soumettre aux entités de gestion et accepter les commentaires soumis par ces entités.

Selon la deuxième méthode, si l'accord de service de l'utilisateur ou les entités de gestion le permettent, l'opérateur pourrait effectuer un test consistant à composer un numéro d'appelant figurant sur la liste des numéros suspects, afin d'obtenir une vérification directe. A partir des résultats de ce test, consignés dans ce qu'il est convenu d'appeler le fichier d'enregistrement vocal, le personnel autorisé chargé de l'audit s'efforcera d'indiquer si l'enregistrement correspond ou non à un spam.

Toutefois, la précision et la qualité de la vérification interactive ont une incidence sur la procédure de contrôle.

Comme indiqué ci-dessus, un leurre peut procéder lui-même à la vérification interactive; en effet, si le résultat du calcul des indicateurs signifie que l'appel sortant est un appel silencieux (voir le § 6.2), le leurre rappellera pour fournir une preuve de la vérification; en revanche, lorsque l'analyse des indicateurs confirme l'existence d'un appel de harcèlement, le leurre établira l'appel téléphonique et l'enregistrera.

Par ailleurs, la coordination entre un groupe de spammeurs envoyant des appels silencieux et une ou plusieurs plates-formes IVR peut induire en erreur les opérateurs quant à l'origine réelle du spam vocal. Il arrive que les plates-formes IVR et les spammeurs envoyant des appels silencieux relèvent d'opérateurs différents. Après avoir enregistré un spam vocal, il serait utile par exemple de suivre la connexion potentielle entre un spammeur envoyant des appels silencieux et une plate-forme IVR en adressant une demande au registre de localisation dans le réseau de rattachement (HLR).

7.2.4 Contrôle

Le contrôle sert à limiter ou à neutraliser/désactiver les appels provenant des spammeurs téléphoniques confirmés comme tels par la vérification, afin de protéger les utilisateurs normaux. Deux méthodes de contrôle sont examinées ci-dessous.

7.2.4.1 Listes blanches/listes noires

La création de listes blanches/listes noires, généralement appelées listes de comptes clés, prend du temps et nécessite une mise à jour constante. Le cycle de vie de chaque élément d'une liste blanche/liste noire doit être géré correctement afin que cette liste reste exacte et efficace. Chaque élément d'une liste blanche/liste noire doit également être dûment tenu à jour de manière sécurisée tout au long de son cycle de vie.

Comme indiqué dans la Recommandation [UIT-T X.1240], la qualité des listes noires varie considérablement, selon le degré de professionnalisme de celui qui les établit. Les listes noires contiennent inévitablement des inexactitudes qui empêchent certains appels légitimes de parvenir à leurs destinataires. Si leur utilisation pose de nombreux problèmes, les listes noires offrent une solution rapide pour refuser la connexion entre les sources de spam vocal et les destinataires (utilisateurs de téléphone).

Les listes noires comprenant des numéros d'utilisateur ou des segments de numéro sont généralement déployées dans un centre de commutation passerelle pour les services mobiles (GMSC), dans des points SCP, des commutateurs ou d'autres entités de réseau. D'une manière générale, les listes noires provenant d'un même opérateur de réseau peuvent être déployées dans des points SCP, des commutateurs ou d'autres entités de réseau, tandis que les listes noires des autres opérateurs de réseau ne peuvent être déployées que dans le centre GMSC dont la capacité en termes de liste noire est parfois trop limitée pour stocker une longue liste de numéros. Une solution simple à ce problème consiste à utiliser des nœuds de signalisation cachés (voir le § 7.2.1.1) derrière le centre GMSC.

Une interaction peut être nécessaire entre les listes blanches et la base de données officielle des appelants déjà identifiés comme légitimes afin d'exclure les appelants véritables imprévus ayant des caractéristiques analogues à celles de spammeurs téléphoniques. Ces appelants peuvent être des centres d'appel, des services de notification ou des services de collecte de commentaires/données, par exemple des rappels de paiement dû, des commentaires sur des projets soutenus par les entités de gestion, des programmes de sensibilisation, des programmes liés à des situations d'urgence ou à des catastrophes, etc.

7.2.4.2 Mécanisme de détermination de l'origine

Le mécanisme de détermination de l'origine permet de déterminer l'emplacement physique réel des spammeurs téléphoniques. Il pourrait parfois être utile d'indiquer l'emplacement ou l'adresse exact du spammeur téléphonique si nécessaire.

Les techniques existantes permettent aux opérateurs de déterminer l'emplacement réel du spammeur téléphonique à partir des informations fournies par le centre de commutation pour les services mobiles (MSC); toutefois, ces techniques permettent uniquement de déterminer une zone approximative. Un emplacement plus précis pourrait être obtenu à partir du service d'informations de localisation de l'opérateur, par exemple un service mondial de géolocalisation assisté.

7.3 Technologies côté utilisateur

Les technologies côté utilisateur devraient compléter efficacement les technologies côté réseau. La mesure des commentaires permet de fournir des informations détaillées sur les spammeurs téléphoniques (comme indiqué au § 7.3.3), ce qui est particulièrement important pour les opérateurs. Les technologies côté utilisateur peuvent nécessiter certaines fonctions particulières de smartphones, dont la prise en charge peut être différente d'un fournisseur à un autre.

7.3.1 Listes blanches/listes noires

Les utilisateurs peuvent utiliser la fonction de commande de connexion des téléphones pour bloquer certains numéros ou segments de numéros considérés comme faisant partie de listes noires, et, parallèlement, cette fonction permettra de mettre systématiquement en relation certains numéros (établis par les utilisateurs ou synchronisés par certaines applications mobiles) lorsqu'ils sont considérés comme faisant partie de listes blanches.

Cette méthode peut fonctionner sur la base des listes blanches/listes noires synchronisées par le côté réseau, tandis que le côté utilisateur dépend généralement des préférences personnelles, car les utilisateurs peuvent tenir leurs propres listes.

7.3.2 Délai d'appel

Le délai d'appel est une technique au niveau de la signalisation qui fonctionne expressément pour les appels silencieux (voir le § 6.2).

Après l'établissement de la liaison de signalisation entre un appelant et un appelé, la sonnerie sera générée périodiquement depuis la liaison. Des appels silencieux seront établis et les utilisateurs recevront un silence ("temps mort") ou une tonalité de courte durée, ce qui indique que l'appel a été abandonné.

Avec un téléphone mobile intelligent, les utilisateurs peuvent bloquer l'appel silencieux au niveau du terminal (côté utilisateur). Etant donné que les utilisateurs peuvent fixer une valeur (seuil) pour la durée de la tonalité de chaque appel entrant au niveau de la couche de signalisation, les appels silencieux peuvent être omis étant donné que la durée de la tonalité est inférieure au seuil. Toutefois, au cas où l'appel normal "à sonnerie brève" serait ignoré, le relevé d'appel sera sauvegardé dans le journal d'appel du téléphone mobile pour permettre à l'utilisateur de procéder à une double vérification.

7.3.3 Commentaires

Après avoir reçu un spam vocal, les utilisateurs peuvent soumettre aux opérateurs des commentaires dans lesquels ils indiqueront le numéro du spam vocal et d'autres informations détaillées. Différents moyens de soumission des commentaires sont possibles, par exemple par SMS, par appel téléphonique, par courrier électronique, voire sur un site web officiel du service client (ou d'autres services équivalents) des opérateurs. Quel que soit le moyen, il devrait être commode et simple pour les utilisateurs de formuler leurs commentaires, par exemple via des applications mises en œuvre dans

les terminaux ou les cartes SIM (module d'identité d'abonné) et les plates-formes de réseau telles que la plate-forme de gestion des dispositifs (DMP) ou la plate-forme hertzienne (OTAP).

En outre, une fois que le service client d'un opérateur a reçu des commentaires, un auditeur autorisé devrait vérifier si les informations communiquées sont réelles et effectives, et appliquer une procédure analogue de vérification interactive avant de prendre les mesures qui s'imposent. S'il existe comme preuve un enregistrement vocal du serveur VMS et si l'accès à l'enregistrement est autorisé par le propriétaire, la vérification pourrait s'avérer plus efficiente et efficace.

7.4 Mécanisme de collaboration

Les opérateurs peuvent, d'entente avec les entités de gestion, d'autres opérateurs ou les utilisateurs, établir un mode de coopération et de communication approprié, afin de lutter contre le spam vocal.

Les opérateurs peuvent établir ou prendre en charge un système de partage d'informations (ISS), qui pourrait servir aux échanges d'informations de base avec d'autres organisations en ce qui concerne les spams vocaux, notamment la liste des spammeurs présumés/vérifiés, la classification des différents spams vocaux, les technologies de lutte contre le spam vocal, etc.

Les entités de gestion peuvent envisager de mettre en œuvre un système ISS et de mettre en place un mécanisme d'échange d'informations, voire d'organiser des réunions officielles à l'intention des opérateurs et des organismes tiers pour échanger les informations les plus récentes.

Les utilisateurs pourraient partager leurs listes noires avec le serveur côté réseau en les téléchargeant. Toutefois, les opérateurs devraient disposer d'un mécanisme de vérification leur permettant de vérifier si un élément figurant dans une liste noire personnelle correspond réellement à un spammeur téléphonique. Les opérateurs devraient prévoir une interface pour le téléchargement des listes noires. Une interaction pourrait être créée entre ce mécanisme et les commentaires des clients. Parallèlement, les entités de gestion devraient vérifier les informations mises à jour pour éviter toute information inappropriée.

Dans le cadre de la mise en œuvre du mécanisme de partage d'informations, les opérateurs peuvent soumettre régulièrement les listes noires vérifiées aux entités de gestion et bloquer les listes noires établies qui sont mises en application par les entités de gestion.

De plus, les entités de gestion peuvent compiler toutes les listes noires qui leur sont adressées par tous les opérateurs et appliquer des mesures et des procédures appropriées. Elles peuvent aussi assumer davantage de responsabilités, par exemple limiter le spam vocal à la source, tout en s'assurant que les opérateurs s'acquittent de leurs obligations.

7.5 Solutions proposées

Utilisée de manière indépendante, aucune des solutions précitées ne peut être entièrement satisfaisante. Pour pouvoir lutter efficacement contre le spam vocal, il convient dans chaque cas de déployer globalement des technologies côté réseau et des technologies côté utilisateur.

On peut intégrer ensemble diverses sources de données dans la procédure d'enregistrement des données de signalisation pour améliorer la précision. Toutefois, une source de données complète serait extrêmement onéreuse à mettre en œuvre.

Il convient d'examiner les situations suivantes.

Les relevés de signalisation SS7 (voir le § 7.2.1) pourraient à eux seuls offrir une solution, dans la mesure où par rapport à d'autres sources de données, le système SS7 permet d'obtenir, sur toutes les liaisons de signalisation, les données les plus utiles pour garantir l'efficacité de la lutte contre le spam vocal.

Par ailleurs, un système de collecte de données fondé sur le réseau intelligent, le service CRBT ou le serveur VMS peut constituer une solution avantageuse, si les opérateurs ont déjà lancé des services

de réseau intelligent, CRBT ou VMS. Toutefois, comme indiqué au § 7.2.1, les sources de données provenant de réseaux CRBT ou IN ne fourniront peut-être pas toutes les données spécifiques requises, et pourraient donc constituer des sources de données complémentaires.

Le modèle proposé au § 7.2.2 est facile à utiliser et n'est pas onéreux; il est aussi couramment déployé pour lutter contre le spam vocal. Pour une analyse plus précise, on pourra utiliser des modèles de règle et des algorithmes plus perfectionnés. Par exemple, des statistiques sur les codes des causes de libération des appels et des statistiques sur les codes des appels rejetés permettraient de restreindre considérablement la liste des numéros suspects.

Toutefois, des modèles de règle ou des algorithmes plus complets risquent de donner lieu à un degré élevé de complexité du système et à des procédures qui prennent beaucoup de temps, d'accroître les délais associés à l'ensemble de la procédure de lutte contre le spam vocal, et, au bout du compte, de se traduire par une satisfaction moindre des clients. Compte tenu de ces considérations, il est essentiel pour les opérateurs de choisir judicieusement les modèles de règle ou algorithmes qui conviennent.

La procédure de vérification interactive peut être différente d'un pays à l'autre. Les entités de gestion peuvent donc aider les opérateurs à établir une procédure de vérification appropriée en fonction des pratiques en vigueur dans leur pays.

Comme il ressort de la procédure de contrôle présentée au § 7.2.4, il vaut mieux intégrer les méthodes côté utilisateur et côté réseau pour réduire le volume de spam vocal. Les services client des opérateurs sont appelés à jouer un rôle important dans la procédure de contrôle et pour répondre aux exigences des clients.

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 partie principale de la présente Recommandation (UIT-T X.1246) et de la 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 CDRn 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 CLIn 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 contribuer à 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 doit 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.

Appendice I

Mesures complètes de lutte contre le spam vocal

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

On trouvera sur la Figure I.1 les approches techniques et non techniques à adopter pour lutter contre le spam. Etant donné que la lutte contre le spam vocal ne se limite pas à un simple problème technique, il convient d'appliquer conjointement diverses approches:

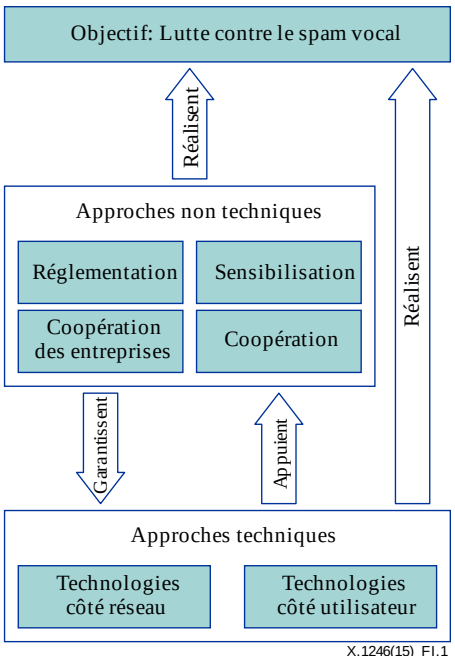

Figure I.1 – Structure de la lutte contre le spam vocal

– La réglementation peut contribuer à protéger les utilisateurs et les opérateurs contre le spam vocal.

– La coopération des entreprises est nécessaire afin que les parties prenantes du secteur privé puissent concevoir et installer divers types de technologies appropriées.

– La coopération peut aider les opérateurs et les entités de gestion à échanger des informations concernant l'adoption effective de la réglementation et les progrès techniques.

– Il est important de sensibiliser les utilisateurs à la nécessité de réduire autant que possible les pertes économiques liées au spam vocal.

Appendice II

Solution proposée pour la vérification interactive

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

D'une manière générale, chaque vérification interactive consiste à composer un numéro d'appelant suspect, à enregistrer la tonalité de retour d'appel avant la connexion et la voix après la connexion, et, enfin, à vérifier le contenu pour déterminer s'il s'agit ou non de spam vocal. Si toutes ces étapes sont réalisées manuellement, cela risque d'épuiser considérablement les ressources humaines des opérateurs. Il convient donc d'envisager une approche optimisée dans un souci de maîtrise des coûts.

La vérification interactive peut être mise en œuvre de manière centralisée pour procéder aux enregistrements et vérifier semi-automatiquement les preuves vocales des spammeurs vocaux présumés, qui seront peut-être isolés les uns des autres et répartis aux quatre coins du réseau.

Dans le cadre de l'approche centralisée, la numérotation et l'enregistrement sont exécutés automatiquement avec de nombreuses opérations en parallèle, et les auditeurs pourront uniquement vérifier les preuves vocales obtenues sans bruit blanc ni autres tonalités de retour d'appel inutiles.

Appendice III

Considérations générales concernant la lutte contre le spam vocal

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Le spam vocal est un outil dangereux utilisé à des fins publicitaires, pour commettre des fraudes et à des fins de harcèlement, etc., et qui est susceptible de se présenter dans les communications au quotidien. Pour lutter efficacement contre le spam vocal, diverses approches doivent être envisagées pour chacun des groupes de participants et divers types de technologies sont décrits dans la présente Recommandation. Les groupes de participants sont les utilisateurs (ou abonnés), les opérateurs, les entités de gestion et les organismes tiers. Le présent appendice décrit plusieurs aspects des groupes de participants à prendre en considération dans la lutte contre le spam vocal.

III.1 Utilisateurs

Les utilisateurs sont les victimes ultimes de la chaîne de communication du spam vocal et ont donc de bonnes raisons de vouloir le blocage du spam. Ils devraient donc mettre en œuvre certaines approches applicables dans le cadre du processus d'ensemble de lutte contre le spam. Les approches suggérées, qui pourront varier en fonction de la situation, sont les suivantes:

– Les utilisateurs devraient si possible installer des applications antispam sur leurs propres dispositifs, par exemple leurs smartphones. Pour une efficacité accrue, les applications antispam doivent être à jour.

– Dès qu'ils reçoivent un spam vocal, les utilisateurs devraient envoyer aux opérateurs de télécommunication ou aux organismes tiers toutes les informations détaillées concernant le spammeur téléphonique.

– Les utilisateurs devraient être beaucoup plus prudents dans leurs communications au quotidien et protéger les informations personnelles, afin qu'elles ne soient pas exposées aux spammeurs.

III.2 Opérateurs

Les opérateurs sont au cœur de la procédure d'ensemble de lutte contre le spam vocal. Étant donné que le spam vocal risque d'amoindrir considérablement les taux de satisfaction des utilisateurs et d'entraîner un gaspillage important des ressources de réseau, les opérateurs devraient être attentifs au problème du spam vocal et mettre en place des méthodes afin de protéger leurs réseaux et de fournir de meilleurs services. Ces approches sont les suivantes:

– Les opérateurs devraient surveiller la totalité du réseau de communication, afin de détecter les spams vocaux potentiels, qui peuvent être à l'origine de transmissions de signalisation ou de profils de trafic anormaux.

– Les opérateurs devraient préinstaller la dernière version des applications antispam dans tous les dispositifs qui pourraient être la cible de spam vocal par le biais de leurs propres circuits de distribution ou de vente. En ce qui concerne les circuits de distribution de tiers, les opérateurs devraient garantir que tous les dispositifs sont parfaitement protégés par des applications à jour.

– Les opérateurs devraient organiser des campagnes de sensibilisation et de formation et encourager les utilisateurs à soumettre des informations détaillées sur les spammeurs téléphoniques aux organismes tiers, par exemple dans le cadre de programmes d'incitation.

– Les opérateurs devraient nouer des alliances avec les entités de gestion et les organismes tiers, afin d'intensifier les efforts pour lutter contre le spam vocal.

III.3 Entités de gestion et organismes tiers

Les entités de gestion et les organismes tiers peuvent superviser ou guider directement les opérateurs, voire fournir l'aide nécessaire.

– Les entités de gestion et les organismes tiers peuvent assurer des formations ou organiser des campagnes de formation et de sensibilisation auprès des utilisateurs et des opérateurs afin de lutter contre le spam vocal.

– Les entités de gestion et les organismes tiers devraient mener des études plus approfondies sur l'évolution du spam vocal et s'efforcer de trouver des approches ou des technologies plus efficaces de lutte contre les formes de spam vocal les plus récentes.

– Les entités de gestion et les organismes tiers devraient dégager les canaux publicitaires ou promotionnels, afin de normaliser l'environnement existant des communications vocales, ou mettre en place une réglementation reposant sur des systèmes reconnus de communications publicitaires pour les entités promotionnelles.

– Les entités de gestion et les organismes tiers devraient communiquer les listes noires les plus récentes aux opérateurs ainsi qu'aux utilisateurs; ces listes noires devraient être tenues à jour avec l'aide des opérateurs et des utilisateurs.

– Les entités de gestion devraient fournir des ressources pour renforcer la lutte contre le spam vocal, dans le cadre de la protection offerte au titre des offres commerciales dont bénéficient les utilisateurs.

Bibliographie

[b-ITU-T E.370] Recommandation UIT-T E.370 (2001), *Principes de service applicables à l'interfonctionnement des réseaux de télécommunication internationaux publics à commutation de circuits avec les réseaux à protocole Internet*.

[b-ITU-T M.60] Recommandation UIT-T M.60 (1993), Termes et définitions relatifs à la maintenance.

[b-ITU-T M.1400] Recommandation UIT-T M.1400 (2015), *Désignations des interconnexions entre opérateurs de réseau*.

[b-ITU-T X.1231] Recommandation UIT-T X.1231 (2008), *Stratégies techniques de lutte contre le spam.*

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

[b-ITU-T X.1245] Recommandation UIT-T X.1245 (2010), *Cadre de lutte contre le spam dans les applications multimédias IP*.

[b-ITU-T Y.1001] Recommandation UIT-T Y.1001 (2000), *Cadre général des réseaux IP – Cadre de convergence des technologies des réseaux de télécommunication et des réseaux à protocole Internet.*

[b-IETF RFC 5039] IETF RFC 5039 (2008), *The Session Initiation Protocol (SIP) and Spam*.

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