Union internationale des télécommunications

# UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

# X.1249

(01/2019)

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 publicitaire sur les applications mobiles

Recommandation UIT-T X.1249

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 | X.1140–X.1149 |
| Protocoles de sécurité (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.1360–X.1369 |
| Sécurité des systèmes de transport intelligents | X.1370–X.1389 |
| Sécurité de la technologie des registres distribués | X.1400–X.1429 |
| Sécurité de la technologie des registres distribués | X.1430–X.1449 |
| Protocoles de sécurité (2) | X.1450–X.1459 |
| ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ | |
| Aperçu général de la cybersécurité | X.1500–X.1519 |
| Echange concernant les vulnérabilités/les états | X.1520–X.1539 |
| Echange concernant les événements/les incidents/l'heuristique | X.1540–X.1549 |
| Echange de politiques | X.1550–X.1559 |
| Heuristique et demande d'informations | X.1560–X.1569 |
| Identification et découverte | X.1570–X.1579 |
| Echange garanti | X.1580–X.1589 |
| 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 oeuvre de la sécurité de l'informatique en nuage | X.1660–X.1679 |
| Sécurité de l'informatique en nuage (autres) | X.1680–X.1699 |

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

# Recommandation UIT-T X.1249

## Cadre technique de lutte contre le spam publicitaire sur les applications mobiles


### Résumé

La Recommandation UIT-T X.1249 propose un cadre technique pour lutter contre le spam publicitaire sur les applications mobiles. Le spam publicitaire sur les applications mobiles désigne l'envoi de publicités non sollicitées, qui s'affichent dans une application mobile. Ces publicités non sollicitées peuvent apparaître sur l'écran du dispositif mobile sous la forme d'un bandeau situé en haut ou en bas de l'écran, d'un interstitiel sur mobile ou d'une superposition. Parallèlement à l'essor rapide des applications mobiles, les publicités sur ces applications ont connu une croissance spectaculaire. Le filtrage des publicités malveillantes peut améliorer l'expérience utilisateur voire la sécurité. Par conséquent, il peut être utile d'établir un cadre pratique pour lutter contre le spam publicitaire sur les applications mobiles, qui intègre autant que possible les avantages de toutes les mesures de lutte contre ce phénomène.



### Historique

| Edition | Recommandation | Approbation | Commission d'études | ID unique* |
|---|---|---|---|---|
| 1.0 | UIT-T X.1249 | 30-01-2019 | 17 | 11.1002/1000/13605 |

### Mots clés

Publicité sur une application mobile, spam.


* 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.

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

## TABLE DES MATIÈRES


| | | Page |
|---|---|---|
| 1 | Domaine d'application | 1 |
| 2 | Références | 1 |
| 3 | Définitions | 1 |
| | 3.1 Termes définis ailleurs | 1 |
| | 3.2 Termes définis dans la présente Recommandation | 1 |
| 4 | Abréviations et acronymes | 2 |
| 5 | Conventions | 2 |
| 6 | Aspects généraux | 2 |
| 7 | Cadre technique | 3 |
| 8 | Composantes fonctionnelles | 3 |
| | 8.1 Composante de prétraitement | 3 |
| | 8.2 Moteurs de filtrage | 3 |
| | 8.3 Moteurs de règles | 4 |
| | 8.4 Plate-forme de vérification | 4 |
| | 8.5 Base de données de spams publicitaires sur les applications mobiles | 4 |
| | 8.6 Plate-forme destinée à recueillir les réactions | 4 |
| 9 | Règles de filtrage | 5 |
| | 9.1 Mots clés | 5 |
| | 9.2 Listes noires/listes blanches | 5 |
| | 9.3 Expression régulière | 5 |
| | 9.4 Détection de caractéristiques | 5 |
| | 9.5 Comportement | 6 |
| | 9.6 Exploration de modèles | 6 |
| 10 | Flux de travail | 6 |
| 11 | Qualité de fonctionnement requise | 7 |
| | 11.1 Précision requise | 7 |
| | 11.2 Efficacité requise | 8 |
| Bibliographie | | 9 |

# Recommandation UIT-T X.1249

## Cadre technique de lutte contre le spam publicitaire sur les applications mobiles

### 1 Domaine d'application

La présente Recommandation fournit un cadre technique de lutte contre le spam publicitaire sur les applications mobiles, qui précise les composantes fonctionnelles, les règles de filtrage et les flux de travail. En outre, dans la présente Recommandation, il est proposé de mettre en place une plate-forme pour recueillir les réactions afin de lutter contre le spam publicitaire sur les applications mobiles.

La présente Recommandation est applicable aux fournisseurs d'applications et aux fournisseurs de services Internet sur mobile.

### 2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation. Au moment de la publication, les versions indiquées étaient en vigueur. Toutes les Recommandation et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références indiquées ci-après. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

Aucune.

### 3 Définitions

#### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

**3.1.1 téléphone mobile** [b-UIT-T X-Sup.19]: appareil électronique utilisé pour faire des appels téléphoniques et envoyer des messages textuels dans un vaste espace géographique par un accès radio aux réseaux publics de téléphonie mobile, tout en permettant à l'utilisateur de se déplacer.

**3.1.2 smartphone** [b-UIT-T X-Sup.19]: téléphone mobile doté de puissantes capacités de calcul, d'une connectivité hétérogène et d'un système d'exploitation évolué qui fournit une plate-forme pour les applications de tierce partie.

**3.1.3 spam** [b-UIT-T X.1242]: diffusion par des expéditeurs à des destinataires, à partir de terminaux tels que des ordinateurs, des téléphones mobiles, des téléphones fixes, etc., d'informations électroniques non sollicitées, indésirables et préjudiciables pour les destinataires.

#### 3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

**3.2.1 filtrage asynchrone**: technique de traitement de fichiers visant à identifier les spams publicitaires, qui permet de traiter simultanément plusieurs fichiers.

**3.2.2 application mobile**: application logicielle conçue pour fonctionner sur des dispositifs mobiles tels que des smartphones et des tablettes.

**3.2.3 publicité sur une application mobile**: publicité diffusée sur une application mobile. Elle peut apparaître sur l'écran du dispositif mobile sous la forme, notamment, d'un bandeau situé en haut ou en bas de l'écran, d'un interstitiel sur mobile ou encore d'une superposition, etc.

**3.2.4 spam publicitaire sur une application mobile**: publicité sur une application mobile qui est généralement non sollicitée, indésirable et nuisible pour le destinataire.

NOTE 1 – "non sollicité" signifie ici "non demandé par l'utilisateur" et "indésirable" signifie que l'utilisateur a fait en sorte d'exprimer clairement son refus, par exemple en désactivant l'option permettant de recevoir certains types de publicité.

NOTE 2 – Le spam publicitaire sur une application mobile est généralement envoyé sans discrimination, en masse et de manière répétitive. La fraude ou le transfert de code malveillant sont des exemples de dommages réels et concrets.

**3.2.5 filtrage synchrone**: technique de traitement de fichiers visant à identifier les spams publicitaires, dans laquelle les fichiers sont traités les uns après les autres.

## 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AD publicité (*advertisement*)

API interface de programmation d'application (*application program interface*)

ID identité

IP protocole Internet (*Internet protocol*)

URL localisateur uniforme de ressources (*uniform resource locator*)

## 5 Conventions

Aucune.

## 6 Aspects généraux

La croissance fulgurante de l'Internet mobile et la nature ouverte des systèmes d'exploitation sur mobile ont entraîné le développement rapide des publicités sur les applications mobiles. En général, pour diffuser des publicités, une application mobile s'appuie sur une interface de programmation d'application (API) fournie par la plate-forme de service. Etant donné que les publicités diffusées sur les applications mobiles sont gratuites ou pour ainsi dire gratuites, elles sont aujourd'hui très prisées. Si la plupart d'entre elles sont légales et conviennent aux utilisateurs, d'autres sont des spams. De nombreuses mesures, telles que les approches "opt-in" ou "opt-out" ont été adoptées en vue de bloquer les spams publicitaires.

Bien que de nombreuses mesures aient été prises pour lutter contre le spam publicitaire sur les applications mobiles, il n'existait toujours pas de cadre technique permettant de lutter contre ce type de publicité sur les applications mobiles. Le spam publicitaire sur les applications mobiles peut avoir de nombreux effets négatifs pour les applications et les fournisseurs de services. Ce type de spam peut consommer une largeur de bande importante pour les données ou occasionner un encombrement du trafic de données, voire entraîner des fraudes sur mobile. Aucune mesure ne s'est révélée parfaitement efficace pour lutter contre le spam. Nous nous proposons donc d'établir un cadre pratique pour lutter contre le spam publicitaire sur les applications mobiles, qui intègre autant que possible raisonnable les avantages de toutes les mesures de lutte contre ce phénomène.

## 7 Cadre technique

Les systèmes de filtrage visant à lutter contre les spams publicitaires sur les applications mobiles (c'est-à-dire les systèmes de filtrage des spams) sont principalement mis en oeuvre sur des plates-formes fournissant des services API aux applications. Celles-ci peuvent s'appuyer sur ces interfaces pour diffuser des publicités et d'autres messages. La Figure 1 décrit le cadre technique de lutte contre le spam publicitaire sur les applications mobiles.

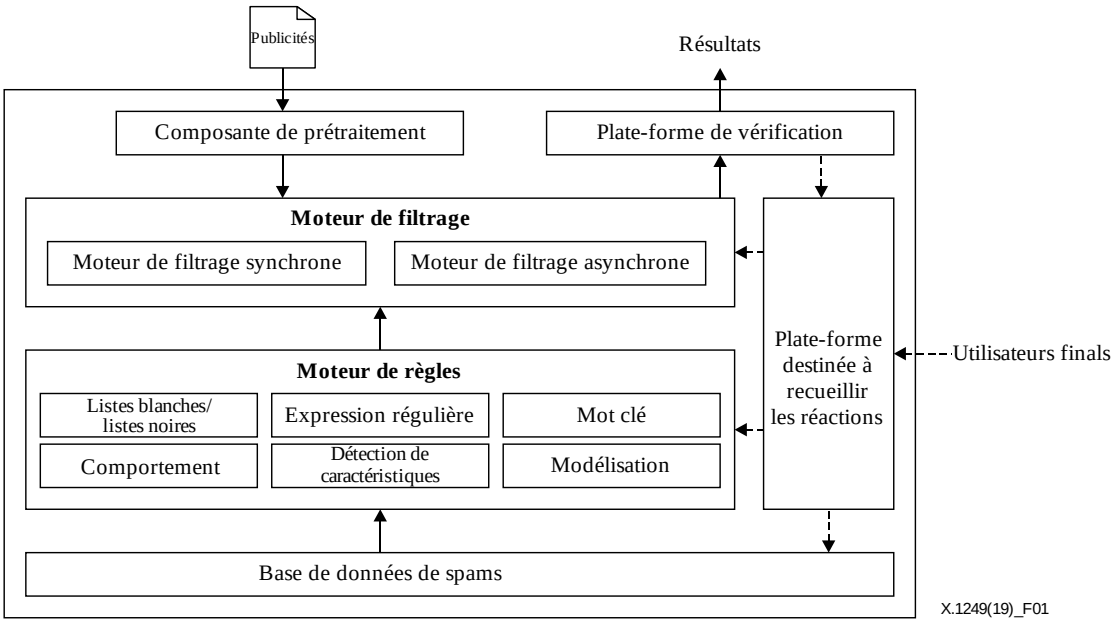


**Figure 1 – Cadre technique de lutte contre le spam publicitaire sur les applications mobiles**

## 8 Composantes fonctionnelles

### 8.1 Composante de prétraitement

La composante de prétraitement est utilisée pour prétraiter les fichiers publicitaires originaux, afin de les convertir au format exigé par les moteurs de filtrage, par exemple en séparant les contenus de texte, d'image, le localisateur uniforme de ressource (URL), ou encore les contenus audio et vidéo.

### 8.2 Moteurs de filtrage

Les moteurs de filtrage sont la composante la plus importante d'un système de filtrage des spams publicitaires sur les applications mobiles. L'objectif principal des moteurs de filtrage est d'identifier les spams publicitaires sur les applications mobiles réels ou potentiels. Les moteurs de filtrage peuvent être classés dans la catégorie de filtrage synchrone ou asynchrone, en fonction des différents moyens utilisés pour identifier les spams publicitaires sur les applications mobiles. Un moteur de filtrage asynchrone est généralement plus efficace en termes de délai qu'un moteur de filtrage synchrone.

#### 8.2.1 Moteur de filtrage synchrone

Le filtrage synchrone attend qu'une règle de filtrage soit terminée avant d'en lancer une nouvelle. Il désigne un filtrage effectué en ligne, en raison de sa complexité moins importante; les résultats du filtrage sont obtenus très rapidement. Normalement, les résultats du filtrage synchrone peuvent être connus immédiatement, ce qui signifie que la décision sera prise dès la fin du filtrage. Si les résultats d'une règle de filtrage ont des conséquences sur l'exécution des règles de filtrage suivantes, il est suggéré de recourir au filtrage synchrone. Le filtrage synchrone peut consister notamment à recourir

à des listes blanches/listes noires, à des expressions régulières, à la modélisation du comportement, ou encore à la détection des caractéristiques.

### 8.2.2 Moteur de filtrage asynchrone

Le filtrage asynchrone permet à différents processus de flux de travail de fonctionner simultanément, ce qui signifie que chaque flux de travail est indépendant des résultats des autres flux. Le filtrage asynchrone désigne un filtrage effectué hors ligne, en raison de la complexité accrue du filtrage des spams publicitaires sur les applications mobiles; généralement, il faut du temps pour obtenir les résultats du filtrage. Le filtrage asynchrone comprend habituellement la reconnaissance audio et vidéo, l'appariement de mots clés, la modélisation profonde, etc.

## 8.3 Moteurs de règles

Les moteurs de règles fournissent les règles de filtrage, à savoir toutes les règles susceptibles d'être utilisées dans les moteurs de filtrage. Les règles de filtrage proviennent de plusieurs sources: configurations des opérateurs, bases de données de spams et règles transmises par des tiers. Le moteur de règles fournit des règles de décision permettant d'identifier les spams publicitaires sur les applications mobiles. Certaines règles de décision seront fondées sur la somme des valeurs pondérées des différents tests d'identification de spam, si les résultats du filtrage ne sont pas déterminés. Le moteur de règles fournira une valeur de seuil (c'est-à-dire une valeur fixe). Si la somme dépasse cette valeur, le moteur de filtrage déterminera si la publicité est ou non un spam. En outre, le moteur de règles peut intégrer différents facteurs de détection issus du moteur de filtrage, afin de déterminer si une publicité est un spam publicitaire sur une application mobile.

## 8.4 Plate-forme de vérification

Tous les spams publicitaires sur les applications mobiles ne sont pas détectables au moyen des moteurs de filtrage. Par conséquent, des méthodes manuelles devraient être utilisées afin d'évaluer ce type de spams, et une plate-forme de vérification devrait être mise en place. Par le biais de la plate-forme de vérification, le vérificateur peut trouver des spams publicitaires sur les applications mobiles inconnus, qui ne peuvent être reconnus par les moteurs de filtrage. La plate-forme de vérification est souvent plus précise que les moteurs de filtrage. Par conséquent, les résultats obtenus grâce à la plate-forme de vérification peuvent être versés dans une base de données de spams publicitaires sur les applications mobiles en vue d'être utilisés ultérieurement.

## 8.5 Base de données de spams publicitaires sur les applications mobiles

Cette base de données sert à stocker les caractéristiques des spams publicitaires sur les applications mobiles. Il s'agit d'une base de données logique qui peut être tenue par chaque fournisseur de services ou partagée par plusieurs fournisseurs de services. Les caractéristiques des spams publicitaires sur les applications mobiles figurant dans la base de données peuvent être utilisées à des fins de comparaison et de filtrage. Le fait d'enrichir cette base de données permet de contribuer à améliorer la performance du moteur de règles. L'extraction des caractéristiques des spams publicitaires sur les applications mobiles nouvellement identifiés au moyen de la plate-forme destinée à recueillir les réactions permet d'enrichir la base de données.

## 8.6 Plate-forme destinée à recueillir les réactions

Les utilisateurs finals sont les cibles, les victimes et les destinataires des spams publicitaires sur les applications mobiles. Tout comme les résultats obtenus via la plate-forme de vérification, la participation des utilisateurs finals est utile pour lutter efficacement contre ce type de spams. Par conséquent, la plate-forme destinée à recueillir les réactions devrait aussi tenir compte des réactions des utilisateurs. Il convient de mettre en place des mécanismes à cette fin, notamment afin de transmettre les réactions à la base de données de spams publicitaires. De telles procédures de traitement des réactions doivent être transparentes et efficaces. En outre, les plates-formes destinées

à recueillir les réactions doivent enregistrer les réactions selon un format normalisé. Cela permettra aux différents opérateurs et entités d'échanger les réactions qu'ils auront recueillies. Les principales adresses des spammeurs pourront être obtenues au moyen de ces échanges, et pourront être ajoutées dans les listes noires.

## 9 Règles de filtrage

### 9.1 Mots clés

Les mots clés sont utilisés pour déterminer si le contenu d'une publicité (c'est-à-dire les mots) correspond aux échantillons enregistrés dans la base de données de spams publicitaires sur les applications mobiles. Les mots clés proviennent des sources suivantes: configuration de l'opérateur, canaux extérieurs, plate-forme destinée à recueillir les réactions et apprentissage machine à partir de bases de données de spams. Les mots clés peuvent servir à identifier de manière précise des publicités malveillantes à haut risque, rapidement et à faible coût; par conséquent, ils sont souvent utilisés pour le filtrage synchrone. Afin de rendre les mots clés plus efficaces, il est nécessaire d'envisager de prétraiter le texte original, afin de filtrer certains caractères volontairement confus, ainsi que différents types de codage des mots clés, en particulier dans le filtrage des URL.

### 9.2 Listes noires/listes blanches

Les listes noires reposent sur le principe de la tenue à jour des adresses ou des domaines IP (protocole Internet) que l'on soupçonne d'envoyer des spams publicitaires sur les applications mobiles. Ces listes peuvent aussi contenir des identités de dispositifs (ID), des URL ou des comptes d'expéditeurs dans la plate-forme de service. Elles peuvent être mises en oeuvre par une entité, afin d'être utilisées en partage, ou être créées et tenues à jour par la plate-forme de service en vue de répondre à ses propres besoins. Le principe des listes blanches consiste à énumérer les sources/entités à l'origine de publicités approuvées ou reconnues. Ces listes peuvent contenir des identifiants de dispositifs ou des comptes d'expéditeurs dans les plates-formes de service. Comme les mots clés, et bien que les listes noires et les listes blanches contiennent inévitablement des inexactitudes, et que les listes noires puissent éventuellement empêcher des publicités autorisées de franchir les barrages mis en place par les moteurs de filtrage, ces deux types de listes constituent des solutions efficaces pour filtrer le spam publicitaire sur les applications mobiles.

### 9.3 Expression régulière

Les expressions régulières sont habituellement utilisées pour correspondre exactement aux publicités malveillantes au format texte et pour les filtrer au moyen de séquences précises. Elles sont souples, logiques et fonctionnelles et aboutissent en règle générale à un résultat final, qui ne nécessite ni appréciation ni modifications additionnelles. Contrairement à un mot clé, une liste noire ou une liste blanche, une expression régulière peut être utilisée pour concorder avec une série de publicités différentes en matière de contenu, mais de forme similaire. Les expressions régulières sont aussi largement utilisées dans le filtrage synchrone en raison de leur efficacité, et du fait qu'une expression régulière, si elle est bien conçue, permet une grande précision. Afin d'éviter toute consommation imprévisible de ressources, les expressions régulières devraient faire l'objet de tests complets avant d'être utilisées, et notamment de tests de performance et de précision.

### 9.4 Détection de caractéristiques

La détection de caractéristiques est une application courante en vision artificielle, qui repose généralement sur la reconnaissance des formes et l'apprentissage machine. L'utilisation la plus représentative de la détection de caractéristiques consiste à reconnaître des publicités malveillantes parmi des milliers d'images. La détection de caractéristiques doit calculer, extraire et stocker les caractéristiques de spams publicitaires sur les applications mobiles connus dans la base de données de spams publicitaires sur les applications mobiles. Lors de la réception d'une image suspecte, la

détection de caractéristiques calcule les informations abstraites de l'image et décide si celle-ci contient une publicité malveillante à ce stade. Les algorithmes d'extraction de caractéristiques et les algorithmes de mise en correspondance associés déterminent si des images publicitaires malveillantes peuvent être trouvées rapidement et avec précision. La détection de caractéristiques aboutit généralement à une conclusion floue, et doit être associée à un processus de prise de décision supplémentaire pour déterminer les résultats finals. En raison de la complexité des calculs et de la comparaison du fichier dans son intégralité, la détection de caractéristiques est plus souvent utilisée pour le filtrage asynchrone.

### 9.5 Comportement

Les spams publicitaires sur les applications mobiles sont le plus souvent envoyés en masse, sans discrimination ou de manière répétitive, et possèdent aussi d'autres caractéristiques particulières. Les moteurs de filtrage peuvent enregistrer des comportements associés aux publicités sur mobile et calculer les relations entre celles-ci. Lorsque le comportement de la publicité reçue cadre avec les caractéristiques déjà stockées dans la base de données de spams, on peut déterminer que le fichier est vraisemblablement une publicité malveillante. Dans la mesure où les comportements des publicités sont aléatoires dans le temps, la détection du comportement pourrait être utilisée pour identifier les publicités malveillantes inconnues, et est plus adaptée au filtrage asynchrone.

### 9.6 Exploration de modèles

L'exploration de modèles est une approche importante qui s'est imposée pour vérifier qu'un modèle satisfait un certain nombre d'exigences. À titre d'exemple, les modèles basés sur les similitudes et sur les arbres de décision sont efficaces pour détecter les spams publicitaires sur les applications mobiles. Parfois, le recours à un seul modèle ne permet pas de déterminer si une publicité est malveillante, alors que l'association de plusieurs modèles, comme dans le cas de l'empilement de modèles, peut être utilisé pour une détection complète. L'exploration de modèles peut être utilisée à la fois pour le filtrage synchrone et le filtrage asynchrone.

## 10 Flux de travail

Le filtrage des spams publicitaires sur les applications mobiles suit généralement le processus décrit dans la Figure 2. Dans certains cas, les moteurs de filtrage synchrone et asynchrone peuvent être utilisés en parallèle.

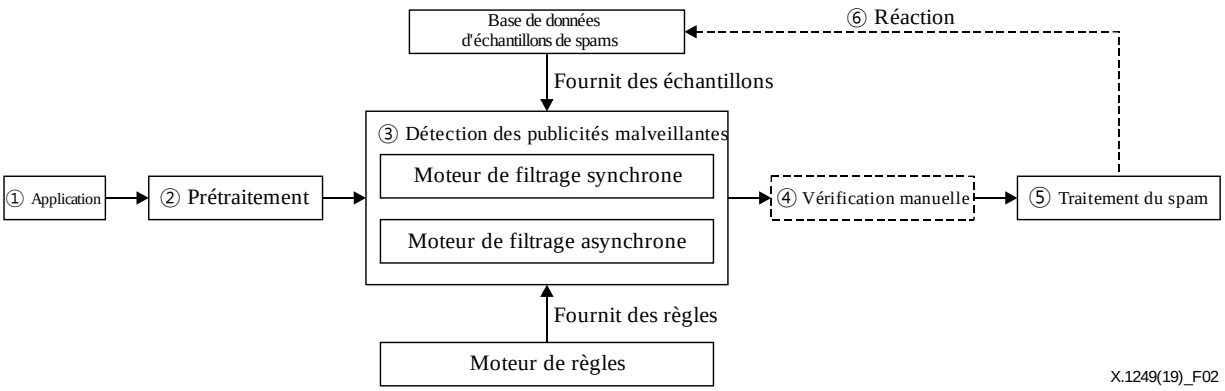


**Figure 2 – Flux de travail pour le filtrage des spams publicitaires**

Les étapes générales sont les suivantes:

1) Les publicités sont fournies aux applications mobiles et diffusées sur celles-ci.

2) Les publicités devraient être traitées au préalable. Par exemple, les différents types de supports média seront subdivisés en URL, texte, audio, vidéo, etc.

3) Selon les menaces et la complexité du filtrage, le contenu sera transmis aux moteurs de filtrage synchrone ou asynchrone, qui sont préconfigurés, mais peuvent être ajustés selon les besoins. Pour procéder à une détection complète, il faut parfois charger le même contenu à la fois dans le moteur de filtrage synchrone et dans le moteur de filtrage asynchrone. Lorsqu'elles sont associées aux règles et aux échantillons fournis par le moteur de règles et par la base de données de spams publicitaires sur les applications mobiles, les publicités sont vérifiées afin de déterminer si un filtrage est nécessaire.

   a) Le moteur de filtrage synchrone détectera les spams publicitaires sur les applications mobiles après l'étape 2, en s'appuyant sur les règles de filtrage du moteur de règles. Si le module de filtrage synchrone trouve un spam publicitaire sur une application mobile, le filtrage de spam sera effectué, la publicité sera bloquée immédiatement et on passera à l'étape 6. Si les URL ou les comptes des applications figurent sur des listes blanches du moteur de filtrage synchrone, la publicité sera directement diffusée. Si les publicités ne peuvent pas être évaluées, il convient de passer à l'étape 4.

   b) Le moteur de filtrage asynchrone détectera les spams présents dans les publicités après l'étape 2, en s'appuyant sur les règles de filtrage du moteur de règles. Si le module de filtrage asynchrone trouve un spam, le filtrage de spam sera effectué, la publicité sera bloquée immédiatement et on passera à l'étape 6. Si les publicités ne peuvent pas être évaluées, il convient de passer à l'étape 4.

4) Il arrive que les publicités doivent être testées et évaluées manuellement. Si un spam est détecté et confirmé, il y a lieu de passer à l'étape 5.

5) Selon la préconfiguration, les spams publicitaires sont traités (enregistrement, remplacement, etc.).

6) Les spams publicitaires sur les applications mobiles sont enregistrés dans la base de données de spams publicitaires sur les applications mobiles. En outre, les spams publicitaires sur les applications mobiles figurant dans la base de données de spams peuvent être extraits pour servir de nouvelles règles et chargés dans le moteur de règles, ou être utilisés pour améliorer ce dernier.

## 11 Qualité de fonctionnement requise

La précision de la détection des spams publicitaires sur les applications mobiles devrait être mesurée au moyen de l'association des taux de faux positifs et de faux négatifs, qui devraient être considérés comme étant équilibrés.

### 11.1 Précision requise

Les taux de faux positifs correspondent au ratio entre le nombre de publicités acceptables qui sont identifiées à tort comme des spams ou des publicités malveillantes, et le nombre total de publicités acceptables. Si le taux de faux positifs est élevé, cela signifie que certaines publicités acceptables sur les applications mobiles ont été bloquées. Par conséquent, il convient de réduire le plus possible les taux de faux positifs.

Les taux de faux négatifs correspondent au ratio entre le nombre de spams publicitaires sur les applications mobiles qui sont identifiés à tort comme des publicités acceptables, et le nombre total de spams publicitaires sur les applications mobiles. Si le taux de faux négatifs est élevé, cela signifie que les utilisateurs seront plus facilement exposés à des spams publicitaires sur les applications mobiles. Par conséquent, il convient de réduire le plus possible les taux de faux négatifs devraient être réduits.

## 11.2 Efficacité requise

L'efficacité d'un algorithme de filtrage des spams publicitaires sur les applications mobiles peut être mesurée au moyen de la complexité dans le temps et l'espace de celui-ci dans le moteur de filtrage. La complexité dans le temps correspond au temps nécessaire pour procéder au filtrage publicitaire, tandis que la complexité dans l'espace correspond à l'espace nécessaire (mémoire). Ces deux indicateurs ont des conséquences importantes sur le type d'application de la règle de filtrage. Des règles de filtrage nécessitant une complexité moindre dans le temps comme dans l'espace peuvent être appliquées dans les moteurs de filtrage synchrone, alors que des règles de filtrage plus complexes peuvent être appliquées dans les moteurs de filtrage asynchrone.

# Bibliographie


[b-UIT-T X.509] Recommandation UIT-T X.509 (2016), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*

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

[b-UIT-T X.805] Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout.*

[b-UIT-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-UIT-T X.1254] Recommandation UIT-T X.1254 (2012), *Cadre de garantie d'authentification des entités.*

[b-UIT-T X-Sup.19] Recommandations UIT-T de la série X – Supplément 19 (2013), *Supplément sur les aspects relatifs à la sécurité des smartphones*.

[b-UIT-T X-Sup.24] Recommandations UIT-T de la série X – Supplément 24 (2014), *Supplément sur un cadre sécurisé de distribution des applications pour les dispositifs de communication*.

## 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 | Equipements terminaux de télégraphie |
| Série T | Terminaux des services télématiques |
| Série U | Commutation télégraphique |
| Série V | Communications de données sur le réseau téléphonique |
| **Série X** | **Réseaux de données, communication entre systèmes ouverts et sécurité** |
| Série Y | Infrastructure mondiale de l'information, protocole Internet, 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, 2019