International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1232

(10/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Countering spam

Technical framework for countering advertising spam in user-generated information

Recommendation ITU-T X.1232

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	**X.1230–X.1249**
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	X.1700–X.1729

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1232

Technical framework for countering advertising spam in user-generated information

Summary

Recommendation ITU-T X.1232 analyses scenarios and characteristics of advertising spam, and specifies a reference framework and process flows to help Internet service providers to counter advertising spam.

It specifies a framework for reducing advertising spam in order to improve the user experience.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1232	2019-10-29	17	11.1002/1000/14085

Keywords

Hybrid authentication, identity-based cryptographic scheme, key exchange, password-based authentication, PKI.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

With the rapid development of Internet business, user-generated information (UGI) has become widely distributed over the Internet, e.g., in community forums, question/answer model services, user-generated audio/video, websites with commentary services, e-commerce evaluation services and live streaming services. UGI can attract advertising spam, disturbing other users' experiences, wasting other users' time and adversely influencing service quality. Countering advertising spam is an urgent requirement for UGI.

Countering advertising spam is critical to the sustainable development of Internet business. However, up to the date of publication, there has been no technical framework standard for countering advertising spam systems in UGI. Therefore, setting up relevant standards to achieve risk control, cleaning up the ecosystem and promoting healthy development of the Internet business are urgent goals.

Recommendation ITU-T X.1232

Technical framework for countering advertising spam in user-generated information

1 Scope

This Recommendation specifies a technical framework for countering advertising spam in user-generated information (UGI). It covers scenarios of advertising spam in UGI, analyses types and characteristics of advertising spam, specifies a user feedback-based recognition mechanism, defines a reference framework and process flows to counter advertising spam.

This technical framework for countering advertising spam mainly focuses on the network service provider side, to allow the best use of network functionalities. Review methods for unknown or suspected spam are outside the scope of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 spam [b-ITU-T X.1242]: The electronic information delivered from senders to recipients by terminals such as computers, mobile phones, telephones, etc., which is unsolicited, unwanted, and harmful for recipients.

3.1.2 spammer [b-ITU-T X.1231]: Spammer refers to the entity or the person creating and sending spam.

3.1.3 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which can result in harm to a system or organization.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASR Automatic Speech Recognition

CASS Countering Advertising Spam Server

ID Identifier

IP Internet Protocol

OCR Optical Character Recognition

SP Service Provider

UGI User-Generated Information

URL Uniform Resource Locator

5 Conventions

None.

6 Scenarios of advertising spam in user-generated information

6.1 Introduction to user-generated information

User-generated information (UGI) comes from voluntarily generation of text, images or media that are presented to other Internet users. UGI can be any form of information created by users of a system or service and made publicly available. Mostly, UGI appears as supplements to online platforms, such as social media websites or e-commerce platforms, and it can take the form of blog posts, wikis, videos or comments.

UGI is used in a wide range of applications, e.g., question-answering applications, news applications, entertainment applications and online video applications. UGI can include text, image, audio, video or their combinations. The quality of UGI is uneven because the Internet threshold is low and open.

6.2 Advertising spam scenarios

Advertising spam in UGI is information that is unwanted or unsolicited by users and has an adverse impact on users' normal access to the Internet.

Spammers can publish advertising spam on websites freely, on the premise that the spammer registers an account on the related website first and then has the right to publish information.

Advertising spam can appear on (non-limiting list) such as:

- e-commerce platforms;
- online video platforms;
- online forums;
- online blogs;
- comment areas of other websites.

7 Types and characteristics of advertising spam

7.1 Common types of advertising spam

7.1.1 Commercial promotion advertising spam

Commercial promotion advertising spam includes retail promotion, product promotion, application promotion and business introduction. This kind of advertising spam usually contains the following keywords in UGI:

- shop name;
- member name;
- product name;
- domain name;
- product link [uniform resource locator (URL)];
- search keywords.

7.1.2 Fraud advertising spam

Fraud advertising spam is advertising spam that has the ability to deceive users and lead to economic loss. For example:

- fake awarding information;
- getting cash from credit card illegally.

7.1.3 Other advertising spam

There are also many other kinds of advertising spam, e.g., meaningless advertising spam.

Meaningless advertising spam refers to chat irrigation with invalid information. It can include meaningless long alphanumeric strings or meaningless special strings.

7.2 Characteristics of advertising spam

7.2.1 Information characteristics

A countering advertising spam server (CASS) can recognize and judge advertising spam according to the information characteristics of UGI, which include but are not limited to:

- keywords, e.g., lottery related information;
- key images, e.g., product images;
- meaningless words and images, e.g., a string of random code characters.

The keywords, key images, meaningless words and images come from the CASS template database.

7.2.2 Behavioural characteristics

A CASS can recognize and judge advertising spam according to the behavioural characteristics of UGI, which include but are not limited to:

- the same user identifier (ID) releases a lot of information in a short period of time;
- a lot of information is published by the same device;
- the same information is published many times;
- the same information is published by many different users;
- different users using the same Internet protocol (IP) address publishes information in a short time.

7.2.3 User feedback characteristics

A CASS can also recognize and judge advertising spam according to suspected advertising spams fed back by many users. The characteristics of these suspected advertising spams include, but are not limited to:

- common words or images extracted from suspected spam information;
- the same suspected spam is fed back by many users.

8 Reference framework

8.1 Framework diagram

Figure 1 shows the reference framework of countering advertising spam in UGI.

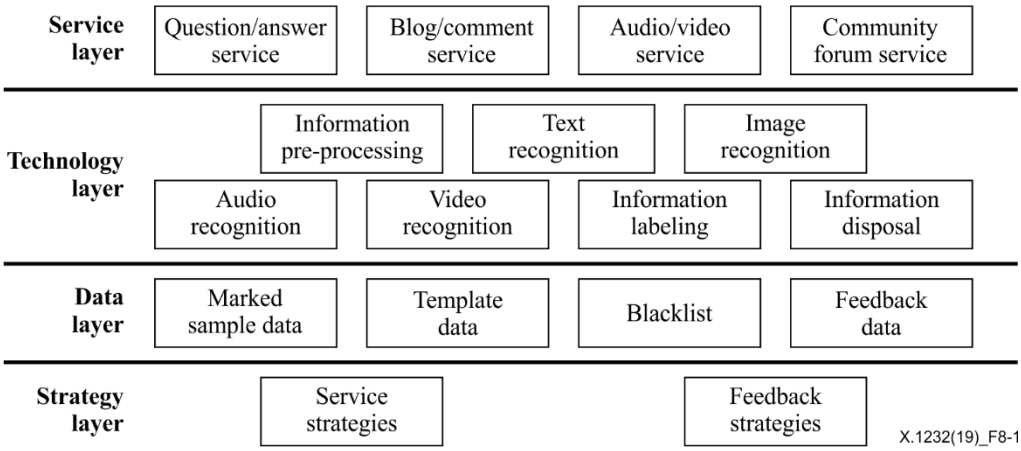

Figure 8-1 – Reference framework of countering advertising spam in user-generated information

There are four layers in the reference framework of countering advertising spam in UGI, which are strategy layer, data layer, technology layer and service layer.

The details of each layer and its functional components are described in clauses 8.2 to 8.5.

8.2 Strategy layer

The strategy layer contains service strategies and feedback strategies.

a) service strategies: the strategies deployed at the service level, e.g., strict authentication, strict information format, flow control support and statistical function provision. Since there are so many different kinds of service with different functions and various vulnerabilities, service strategies for countering advertising spam in different services differ from each other;

b) feedback strategies: end-users are the final receivers of spam, the possible victims of viruses and scams. The participation of end-users is helpful for countering spam effectively and efficiently. Therefore, feedback from end-users should be taken into account when developing solutions for countering spam. However, end-user participation shall be on a voluntary basis. The service provider (SP) should provide a platform and standard formats for spam feedback.

8.3 Data layer

The data layer focuses on forming a database of different kinds of data that can be helpful to judge advertising spam. It includes marked sample data, template data, blacklist or whitelist and custom rules.

a) marked sample data: the data tagged by a person or system. Through feature extraction and deep learning for similar tag data, data with the same features can be extracted as template data;

b) template data: includes advertising spam template, which can be used for comparison to judge advertising spam;

c) blacklist: includes an account list, device ID list, mobile number list or IP list. A CASS can deal with UGI according to a blacklist. For example, if an account that is on the blacklist releases information, that information is checked;

d) feedback data: includes data from user feedback.

8.4 Technology layer

8.4.1 Information pre-processing

Information pre-processing processes UGI in coarse-grained solutions to provide data for other recognition modules. It includes the following functions:

- data clarification: text information clarification, image type classification, effective voice filtering, etc.;
- data validation: text grammar check, graphic correlation assessment, search correlation assessment, etc.;
- data extraction: specific picture capture, optical character recognition (OCR), text keyword extraction, speech to text, etc.

8.4.2 Text recognition

Text recognition can be used to judge advertising spam by keyword extraction, deep learning and semantic analysis. It includes the following functions:

- keyword or similar information comparison: comparing the text to be recognized with the keyword or similar information in the template data;
- text noise reduction: eliminating special symbols, emoji, non-text characters between texts;
- text correction: word calibration, near word calibration, split word and combination word calibration, etc.;
- recognizing the positive or negative emotions expressed by sentences;
- extracting subject, predicate and object from sentences;
- text classification: using deep learning to classify text information into different types, e.g., commercial promotion or fraud;
- distinguishing Chinese, English, Arabic, French and other languages in the text;
- text aggregation: associating similar text in different data sets together.

8.4.3 Image recognition

Image recognition can be used to judge advertising spam by deep learning and other technologies. It includes the following functions:

- image size normalization: compressing or enlarging a picture with too large or too small pixels into a fixed size image;
- target image detection: capturing the target image from UGI, e.g., logo, special character or product;
- image feature extraction: image feature can reflect the essential characteristics of the image, which can be used for image matching;
- comparing the extracted image feature with template data and calculating the similarity, then sorting the similarity and retrieving the image with the highest similarity;
- image classification: using deep learning to classify image information into different types, e.g., commercial promotion or fraud.

8.4.4 Audio recognition

Audio recognition can be used to judge advertising spam by converting audio to text, keyword extraction, deep learning and other technologies. It includes the following functions:

- voiceprint recognition: 1:1 voiceprint comparison, 1:N voiceprint search, non-semantic voice recognition;
- long form automatic speech recognition (ASR): converting long form audio into text to provide a basis for information processing and data mining;
- audio classification: classifying different audios into different types, e.g., commercial promotion or fraud.

8.4.5 Video recognition

Video recognition can be used to recognize advertising spam in video and live frame. It includes the following functions:

- video decoding: decoding the video stream and cutting the frame into a set of image sequences with time stamps;
- image feature extraction: extracting a series of image features from the set of decoded image sequences;
- multi-modal feature fusion: restructuring the image feature corresponding to the image sequence and turning the feature sequence into a feature by using the feature fusion model;
- video classification: classifying different video into different types, e.g., commercial promotion or fraud.

8.4.6 Information labelling

Information labelling can label recognized advertising spam information, e.g., with the type of the information. It includes the following functions:

- removing the same image in the data set;
- removing the same text in the data set;
- sorting and filtering the labelled information.

8.4.7 Information disposal

Information disposal deal with advertising spam based on the disposal strategy. Different services in different organizations may have different disposal strategies. For example:

- deleting advertising spam directly from the associate platform or website;
- blocking access to advertising spam;
- adding the spam account to a blacklist;
- limiting the permission of the account;
- lowering the permission level of the account.

8.5 Service layer

The service layer may include question/answer service, blog/comments service, audio/video service, and community forum service.

a) question/answer service: in which the user can ask questions and provide answers. Inside the questions or answers, user may insert advertising spam;

b) blog/comment service: in which the user can publish blogs or comments, possibly including advertising spam;

c) audio/video service: in which the user can upload user-generated audios or videos, possibly including advertising spam;

d) community forum service: in which the user can exchange information in a community forum, possibly including advertising spam.

Note that these services are examples only, and the list is not exhaustive.

9 Process flows

9.1 Advertising spam recognition flow

Figure 9-1 depicts the advertising spam recognition flow.

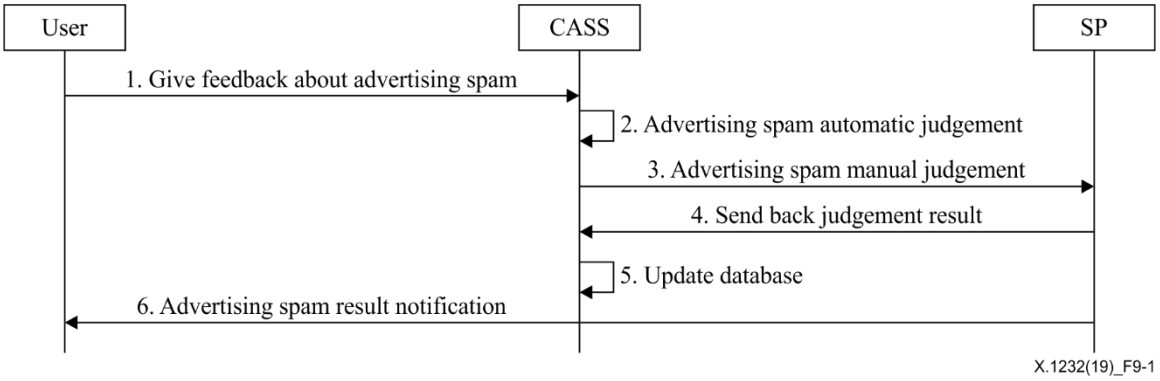

Figure 9-1 – Advertising spam recognition flow

The advertising spam recognition flow includes the following steps:

Step 1: User gives feedback about advertising spam to a CASS when user finds advertising spam information.

Step 2: The CASS automatically judges advertising spam when receiving feedback from users.

Step 3: If the CASS cannot make a decision about advertising spam, it sends a request to the SP for manual judgement.

Step 4: After judging the advertising spam manually, the SP sends the judgement to the CASS.

Step 5: The CASS records the judgement and updates the database accordingly.

Step 6: The SP sends the judgement of the advertising spam to the user.

9.2 Advertising spam processing flow

Figure 9-2 depicts the advertising spam processing flow.

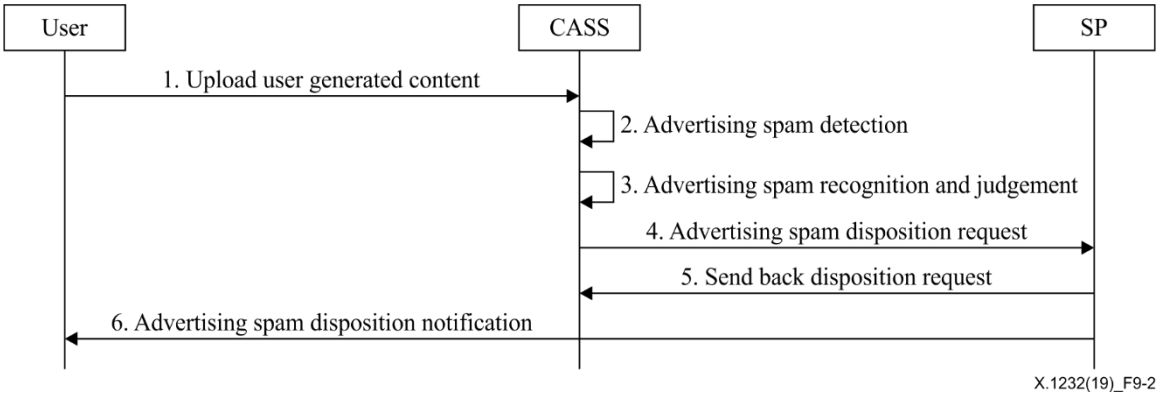

Figure 9-2 – Advertising spam processing flow

The advertising spam processing flow includes the following steps:

Step 1: The user uploads UGI to a CASS.

Step 2: The CASS detects advertising spam when receiving information from the user.

Step 3: The CASS performs advertising spam recognition and produces a judgement when it detects suspected information.

Step 4: When the CASS finds advertising spam, it sends a request to the SP for disposition.

Step 5: After processing the advertising spam (e.g., labelling, deletion, blocking), the SP sends back the disposition result to CASS.

Step 6: The SP sends an advertising spam disposition notification to the user.

Bibliography

[b-ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam*.

[b-ITU-T X.1242] Recommendation ITU-T X.1242 (2009), *Short message service (SMS) spam filtering system based on user-specified rules*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020