International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1233

(09/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Countering spam

Guidelines for countering spam over instant messaging

Recommendation ITU-T X.1233

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	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
IMT-T SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1233

Guidelines for countering spam over instant messaging

Summary

Recommendation ITU-T X.1233 establishes guidelines for instant messaging (IM) service providers (SPs) and users to counter spam over instant messaging (SPIM) and to reduce propagation of SPIM in cyberspace and improve the IM user experience.

This Recommendation analyses scenarios of SPIM generation in IM, specifies technical measures and mechanisms to counter SPIM for IM SPs, and establishes guidelines to counter SPIM for IM users.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1233	2021-09-03	17	11.1002/1000/14773

Keywords

Countering SPIM, guidelines, IM service provider, IM user.

[*] 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

The popularity of instant messaging (IM) applications has resulted in instant messaging (IM) applications becoming an important way to spread spam, along with voice, short message service (SMS) and email. With real-time and efficient message transmission, IM allows great convenience in social contacts. However, it also opens the door for spammers to send spam over instant messaging (SPIM). The volume of spam advertisements, pornography and other illegal information, such as phishing information, viruses, Trojan worms and spyware, sent by IM is growing exponentially. This is not only harassing or even incurring economic losses to uses, but also seriously affecting the security of cyberspace. Countering SPIM has become a significant element in counteracting spam.

There remains, however, a lack of guidance for service providers (SPs) and users who wish to counter SPIM while operating or using IM. This means that efforts to counter SPIM have not been effectively managed. It is therefore urgent to build relevant standards to guide IM operators and users in techniques and management measures that can prevent SPIM.

Recommendation ITU-T X.1233

Guidelines for countering spam over instant messaging

1 Scope

This Recommendation establishes guidelines for IM service providers (SPs) and users to counter spam over instant messaging (SPIM). It covers IM spam scenarios, technical measures and mechanisms to counter SPIM for IM SPs, emergency response disposal measures to counter SPIM for IM users, etc.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 spam over instant messaging (SPIM) [b-ITU-T X.1244]: A spam targeting users of instant messaging service.

NOTE – For the purposes of this Recommendation, no term "spam" is defined.

3.1.2 spimmer [b-ITU-T X.1244]: Sender of SPIM.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 instant messaging (IM): An exchange of content between a set of participants in near real time. Generally, the content is short text messages, although that need not be the case.

NOTE – Based on [b-IETF RFC 3428].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IM	Instant Messaging
IP	Internet Protocol
NE	Network operator
SMS	Short Message Service
SPIM	Spam over Instant Messaging
SP	Service Provider

5 Conventions

The verbal form "shall" indicates a requirement strictly to be followed in order to conform to this Recommendation.

The verbal forms "should" and "should not" indicate that, among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others; that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain possibility or course of action is deprecated, but not prohibited.

The verbal form "can" indicates an optional requirement that is permissible. This term is not intended to imply that the implementation must provide the option.

6 Spam over instant messaging scenarios

SPIM is becoming a major challenge for IM services. SPIM affects the performance of IM systems in various ways, such as wasting resources, including memory, central processing unit, storage space and bandwidth resources, and may cause major problems such as the spread of worms and denial of service attacks. SPIM scenarios include but are not limited to the following,

- Utilization of automated means to register a large number of accounts for nefarious purposes, such as spreading of SPIM.
- Use of an account without authorization of the account owner to establish a session connection with the target user to spread SPIM.
- The lack of built-in security mechanisms, such as a lack of a confirmation mechanism when adding friends, creates an environment in which SPIM can spread quickly.
- Disclosure of messages over an unsecured delivery channel. Hackers can tamper with instant messages during transmission. Advertisements or malicious codes may be inserted in the message, converting the message to SPIM.
- Manufacturers acting illegally push SPIM subscriptions to users for commercial benefit.

7 Guidelines for IM service providers to counter SPIM

7.1 Configuration of anti-SPIM functions

The IM SP shall provide anti-SPIM functions while providing IM service. Anti-SPIM functions should include but are not limited to the following:

- automatic user registration detection and control;
- authorization control when adding friends;
- message-sending rate detection and limitation;
- message filtering based on blacklists;
- user complaint platform that among other functionalities has a simple feedback mechanism to alert an IM SP about SPIM received.

At the same time, the IM SP shall maintain anti-SPIM functions in the process of operation. Scenarios should include but are not limited to the following:

- maintaining anti-SPIM databases, such as friend lists and blacklists, so that they are available and stable;
- maintaining user complaint information to enhance the accuracy of this information;
- adjusting thresholds used in anti-SPIM functions, such as those for message-sending rate restriction and number of complaints that an account can receive before being added to a blacklist.

7.2 Behaviour monitoring and control

The IM SP shall take measures to monitor the following behaviours and to generate alarms when anomalies are detected. Behaviours that should be monitored include but are not limited to the following.

- Authentication failure behaviour. For example, a number of authentication requests are sent from the same Internet protocol (IP) address. If there are lots of such behaviours, it might be that a spimmer is stealing accounts to send SPIM. This should trigger an alarm and subsequent authentication requests from that IP address should be dropped.
- Malicious complaint behaviour. For example, an account submits a large number of complaints in a certain period of time, whether the complaints concern different accounts or the same account, if the number of the complaints exceeds a certain threshold, it should trigger an alarm and the complaints from the account should be ignored, thus improving the accuracy of complaints.
- Malicious addition of accounts to blacklists behaviour. For example, if some accounts add a specific account to a blacklist, it should be detected whether those accounts are on a suspicious account list. If most of them are on a suspicious account list, an alarm should be triggered. These attempts to blacklist the specific account should not be considered when counting the number of times the specific account has been added to a blacklist, thus improving the accuracy of the blacklist.

7.3 Auditing and recording

IM SPs shall adopt technical measures for auditing and recording user behaviours and cybersecurity incidents to counter SPIM. The records that the IM service should audit include but are not limited to the following.

- User behaviour logs, including registration behaviour information and user authentication information. For example, the IM SP should record the user's historical actions (e.g., message-sending behaviours exceeding the threshold of message-sending rate restrictions and malicious complaint behaviours). The message-sending behaviour logs should include but are not limited to the following information: sender's account information (e.g., IP address, username, whether the sender is included on a suspicious list or blacklist list), recipient's account information, relationship type between the sender and recipient (e.g., friends, non-friends, friend members in a group, non-friend members in a group, friends of other IM systems and phone contacts). IM server providers should integrate analysis of this information to identify suspicious or malevolent activities. Malicious complaint behaviour logs should include but are not limited to the following information: complainer account's information (e.g., IP address, username, whether included on a suspicious list or blacklist list), information of the account being complained about, and number of complaints in a certain period of time. If the number of complaints exceeds a threshold, the complaints from the complainer's account are ignored, thus improving the accuracy of the complaint platform.
- SPIM filtering record, which includes SPIM filtering behaviours and the filtered message. A SPIM filtering behaviour record should include but is not limited to the following information: the sending account of the filtered message (e.g., IP address, username, whether on a suspicious list or blacklist list), which filtering measures are being used (e.g., filters based on blacklists, sending rate control or authorization control). The filtered message should be recorded so that it can be resent if it is mistakenly filtered.

7.4 Emergency response

An IM SP should formulate an emergency response plan for major SPIM events.

Major SPIM events should be covered by an emergency response plan, which should include but is not limited to the following:

- anti-SPIM database of IM server is modified, invaded or controlled;
- SPIM complaint platform is modified, invaded or controlled;
- threshold of an automatic registration function is illegally modified;

- large-scale complaints against SPIM are launched in a given period of time.

An IM SP should determine the type and level of each of these SPIM events according to the actual situation, and formulate an emergency response process and emergency operation guidelines for each type and each level of SPIM event.

An IM SP should establish a monitoring and warning mechanism for major SPIM events, discover major SPIM events and notify relevant personnel in a timely fashion.

An IM SP should also summarize the causes of major SPIM events after an emergency response, evaluate the effectiveness of emergency response measures and rectify the problem in a timely fashion.

7.5 Risk assessment management

IM SPs should assess risk of the likelihood and severity of SPIM events. Risk management should be integrated within basic operating activities, flowing from the management assessment, cascading to security assessment and functional assessment. Risk assessment management should include but is not limited to the following.

- An IM SP should conduct a management assessment that should include, for example, developing an anti-SPIM policy and monitoring whether security compliance processes and strategies are in place to mitigate the risk of SPIM; additionally, it should facilitate the implementation of the policy. An IM SP should also review and update the current risk assessment policy and procedure according to an organization-defined frequency or whenever there are significant changes to the IM system or operation environment.
- An IM SP should conduct a security assessment that should include, for example, automating the vulnerability management process by using standards (e.g., enumerating application flaws and improper configurations, and formatting checklists and test procedures) to identify what is most the likely cause of SPIM (e.g., password vulnerabilities, unsecure firewall settings and Trojan worms), and quantify the predisposing conditions for major SPIM events.
- An IM SP should conduct functional assessment that should include, for example, discovering illogical processing and cascading errors that can lie within an IM system's code (e.g., automatic user registration, unlimited user sending rate within a given period of time, lack of built-in security mechanisms and revealing messages over an unsecured delivery channel) when the IM system upgrades.
- An IM SP should assess risk regularly or review and update its risk assessment policy as necessary. Risk assessment should comprise three interrelated components: management, security and functional assessments. For example, management and security assessments should be carried out together with the general risk assessment, functional assessment should be carried out before an IM system upgrade, during a IM system upgrade or both. At the same time, an IM SP should either remediate legitimate flaws in organization-defined response times or implement controls to prevent the spimmer exploiting the vulnerability.

7.6 Security protection measures

An IM SP should take security protection measures to counter SPIM. The security protection measures should include but are not limited to the following.

- An IM SP should deploy anti-distributed denial of service attack measures to protect the blacklist library, complaint platform, security monitoring and audit methods and to improve the availability of anti-SPIM functions.
- An IM SP should deploy anti-virus, anti-Trojan and anti-worm measures to prevent the server from being infected and controlled by spimmers who would modify anti-SPIM configurations or disable anti-SPIM functions and then send SPIM.

- An IM SP should implement multiple access control methods in network boundaries, systems and applications of the IM system, to prevent unauthorized access by spimmers who would modify anti-SPIM configurations or disable anti-SPIM functions and then send SPIM.
- An IM SP should deploy intrusion detection and protection methods to detect network attacks and prevent the IM system from being intruded into by spimmers who would modify the configuration or disable anti-SPIM functions and then send SPIM.

8 IM users functionality to support anti-SPIM

An IM user should have the possibility to configure the IM client to guard against SPIM when using an IM system. The configuration should include but is not limited to the following. An IM user should have the possibility to:

- use a verification confirmation mechanism, including confirmation of authentication requests and confirmation of additions to the group, to ensure that all actions are approved by the user.
- configure settings to not allow receipt of messages or files from unauthorized users.
- configure a blacklist in a timely fashion, and not allow receipt of messages or files from suspicious accounts.
- use a strong password and change it regularly to prevent the account being stolen and used to send SPIM.
- monitor the execution of privileged functions, and disable and alter implemented settings as they may cause SPIM (e.g., accepting a stranger's authentication request).

9 Guidelines for service providers or network operators to counter SPIM

Service providers or network operators (SPs/NEs) can help to counter SPIM by means such as building a unified SPIM complaint platform, building a unified blacklist database to prevent SPIM, testing and verifying anti SPIM functions of an IM system, and providing SPIM detection services for IM SPs. This includes but is not limited to the following.

- SPs/NEs should build a unified complaint platform for multiple IM services. The complaint platform can accept complaints from users about an account sending SPIM, and classify complaints according to different IM services. When the number of complaint users against an IM account reaches a certain number, details of the IM account are sent to the corresponding IM service blacklist database.
- SPs/NEs should build a unified blacklist database for multiple IM services. The blacklist database is synchronized with the blacklist database of each IM service in the network. There are two sources for a blacklist, accounts included in the database that are:
  - the subject of complaints through the above complaint platform;
  - detected to be sending SPIM through the SPIM detection service.
- SPs/NEs should provide a regular dial test verification service for an IM SPs, preventing anti SPIM functions in an IM system from being turned off, which may be caused by hacker attack. If the corresponding function is not turned on after verification, an SP/NE can send an alarm to the IM SP. Dial test verification functions include but are not limited to the following, simulation of:
  - automatic registration behaviour, and verification of whether the IM system can identify and prevent automatic registration;
  - an account sending multiple messages in a unit of time (the number of messages exceeds the threshold set by the IM system), and verification of whether the IM system can detect and discard messages sent by the account subsequently;

  - a blacklisted account sending a message, and verification of whether the IM system can discard messages sent by the account;
  - malicious complaints and verification of whether the IM system can identify and discard them.
- SPs/NEs can provide a SPIM detection service for an IM SP. They should sign a service level agreement with each IM SP, which should include confidentiality terms, to protect the privacy of users. The process of detecting SPIM SPs/NEs is as follows:
  - to deploy detection systems at key nodes in the network, and detect the IM message packet header under the authorization of an IM SP;
  - to analyse the behaviour of sending multiple IM messages by an IM account – if the number of messages sent by the IM account within a certain time range exceeds a certain threshold, it can be determined that the account is sending SPIM;
  - to discard IM messages sent by the account mentioned previously directly;
  - to include the account mentioned previously in the blacklist database.

Through a SPIM detection service provided by SPs/NEs, SPIM can be found and discarded at the near edge, which can not only save network bandwidth, but also avoid consumption of IM server resources.

Bibliography

[b-ITU-T X.1244]	Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.
[b-IETF RFC 3428]	IETF RFC 3428 (2002), *Session initiation protocol (SIP) extension for instant messaging*. Available [viewed 2021-10-09] at: https://tools.ietf.org/html/rfc3428

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, 2021