International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1248

(09/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Countering spam

Technical requirements for countering instant messaging spam

Recommendation ITU-T X.1248

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 legder technology security	X.1400–X.1429
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

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

Recommendation ITU-T X.1248

Technical requirements for countering instant messaging spam

Summary

Recommendation ITU-T X.1248 identifies characteristics of spam over instant messaging (SPIM) and specifies technical requirements for countering it. As instant messaging (IM) increases in popularity, the proliferation of SPIM becomes an increasingly serious problem. The characteristics of IM, such as being Internet protocol (IP)-based with widespread usage that is free of charge, potentially allows SPIM to spread widely and uncontrollably. If SPIM problems are not carefully addressed, they can have negative impacts on the utilization of the IM service itself.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1248	2017-09-06	17	11.1002/1000/13262

Keywords

Instant messaging spam, SPIM.

---

* 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/.

© ITU 2017

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Introduction

With the rapid development of the Internet and mobile Internet, instant messaging (IM) has grown from being a simple chat tool to an integrated information platform that integrates communication, information, entertainment, search, e-commerce, business collaboration and enterprise customer services as a whole. Because of its low price and ease of use, more and more people are switching to IM, thus having a huge impact on traditional communication fields. Currently, telecom operators are increasingly providing IM services; but at the same time, IM has become critically subject to spreading spam on voice and short message service (SMS) services. Telecom operators around the world are aware of and/or impacted by spam over instant messaging (SPIM) to varying degrees. SPIM not only wastes network resources, but also causes loss of time and productivity of users. In addition, SPIM is used for phishing, and spreading viruses, worms, spyware and other forms of malware, and can even carry harmful information offensive to users. Thus, SPIM reduces user satisfaction in using IM and has become an important factor hindering the usage of IM.

Although many anti-spam countermeasures have been implemented on IM systems, many weaknesses in IM systems still exist that may cause SPIM, such as: unlimited registration rate, lack of confirmation when receiving messages, insecure network transmission mechanisms, lack of message sending rate controls for users, inevitable vulnerabilities in IM systems.

This Recommendation specifies technical requirements for countering SPIM in view of functions of an IM system, in order to stop the production and propagation means of SPIM. For example, it is important to require that a registration mechanism be designed to prevent mass automated registrations, and that the IM system provides users the function of choosing whether to receive or block all messages from authorized/unauthorized entities, and to limit a user's sending rate if they have exceeded a normal threshold.

Recommendation ITU-T X.1248

Technical requirements for countering instant messaging spam

1 Scope

This Recommendation identifies types and characteristics of spam over instant messaging (SPIM). In order to mitigate the production and propagation of SPIM, this Recommendation specifies technical requirements for countering SPIM, involving both the instant messaging (IM) client and the IM server. This Recommendation mainly focuses on anti-SPIM measures of the IM system layer, and is applicable for IM service operators.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 instant messaging (IM) [b-IETF RFC 3428]: 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.

3.1.2 spam [b-ITU-T X.1240]: The meaning of the word "spam" depends on each national perception of privacy and what constitutes spam from the national technological, economic, social and practical perspectives. In particular, its meaning evolves and broadens as technologies develop, providing novel opportunities for misuse of electronic communications. Although there is no globally agreed definition for spam, this term is commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging for the purpose of marketing commercial products or services.

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

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ID Identity

IM Instant Messaging

IP Internet Protocol

SMS Short Message Service

SPIM Spam over Instant Messaging

5 Conventions

None.

6 Characteristics and generation scenarios of SPIM

SPIM refers to an instant message that is received by a user, which is perceived as being unwanted or as causing disruption to that user. Thus, SPIM has the following characteristics:

– SPIM usually occurs in real-time. In the case where both the sender and the receiver are online, SPIM is received at almost the same time as it is sent. Even if the receiver is not currently online, SPIM can be immediately received after the receiver comes online;

– SPIM is often sent in bulk, thus a large number of messages, with the same content, are transmitted concurrently;

– Spimmer is the term used to define an unauthorized sender of SPIM to IM recipients. However, at times, a friend's account may be compromised and instructed to send SPIM due to an infection by malicious code or due to disclosure of account and password information. SPIM sent by friends is more deceptive, especially when it contains links to malicious websites or executable files which most recipients will click on and thus their systems will more likely be infected with malicious code;

– SPIM cannot easily be traced since accounts can be arbitrarily created, and usually are not traceable to a real identity.

The generation of SPIM is closely related with IM system functions (refer to Appendix I), and the scenarios that may generate SPIM are as follows:

– Spimmers can use automatic registration software to register a large number of accounts, and use these accounts to spread SPIM;

– Malicious users may use false IM accounts, and can use these false accounts to send SPIM;

– If a malicious attacker has obtained control of a legitimate user account without authorization, they can modify the user's information such as password, or other authentication information, to use of this account (often for a long time) to send SPIM;

– If an IM client's receiving parameter is modified without authorization, SPIM could be received without any limitation;

– Instant messages can be tampered during transmission. Advertisements or malicious code may be inserted into an IM and turn it into SPIM;

– Due to the lack of confirmation mechanisms, a spimmer can be free to add friends, and to send SPIM to those friends.

For the prevention of SPIM, it is necessary to fully consider the characteristics of SPIM and the scenarios that may cause SPIM, in order to take comprehensive preventive measures.

7 Functional IM architecture for countering SPIM

7.1 Overview

The functional IM architecture for countering SPIM is depicted in Figure 7-1.

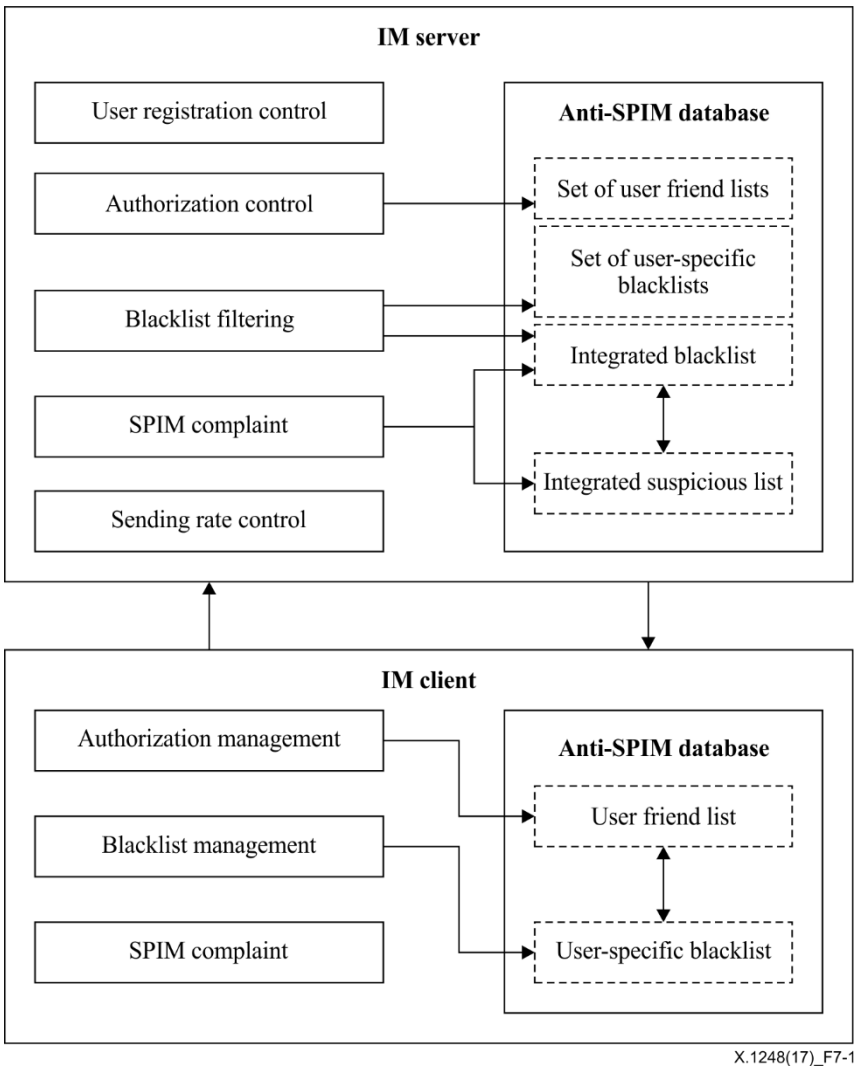

Figure 7-1 –Functional IM architecture for countering SPIM

This architecture integrates functionalities to counter SPIM, including blacklist filters, user registration controls, and SPIM complaint. More importantly, the architecture supports filtering based on limiting the IM sending rate, and controlling authorization of the IM sender.

Appendix I describes, in greater detail, the IM client and IM server functionalities, and the roles of the IM sender, IM receiver and spimmer.

7.2 Components functionality

7.2.1 IM server

The IM server component functionality includes the following six elements:

1) User registration control

   It is required to use manual confirmation methods, such as verification codes, e-mail verifications, SMS verification codes, to prevent users from automatic registration. This would prevent spimmers who have a large number of automatically-registered accounts from sending SPIM.

2) Authorization control

   It is required to forward a user's request to add a friend, and to authorize the friend's relationship with the user based on the IM client's feedback.

3) Blacklist filtering

It is required that the IM server filters instant messages based on an integrated blacklist and a set of user-specific blacklists.

4) SPIM complaints

It is required that users' complaints about accounts which send SPIM are accepted, and to determine whether to add these accounts to the integrated suspicious blacklist or the integrated blacklist. It is required to interface with external SPIM complaints-handling systems, and to import and export the integrated blacklist.

5) Sending rate control

It is required that the number of instant messages, sent by the same account within a given period of time, is controlled. The instant messages exceeding this threshold should be suppressed.

6) Anti-SPIM database

- Set of user friend lists: It includes friend lists of all users managed by the IM server. It is required that the user friend list set in the IM server, is synchronized with the user friend lists in the IM clients.
- Set of user-specific blacklists: It includes user-specific blacklists of all users managed by the IM server. It is required that the user-specific blacklist set is synchronized in the IM server with user-specific blacklists in the IM clients.
- Integrated blacklist: It includes accounts contained in complaints reported by users, and accounts detected by the IM server. For example, when an IM user's rate of messages sent exceeds a given threshold, the sender's ID shall be classified and added to the integrated blacklist by the IM server. The integrated blacklist also includes accounts that are imported from other systems, such as other IM servers.
- Integrated suspicious list: It is required that a list of all suspicious accounts managed by the IM server be generated. The integrated suspicious list can be developed via user complaints, importing from other systems, etc.

7.2.2 IM client

The IM client component functionality includes the following four elements:

1) Authorization management

Two key components that should be included are visibility control for IM identity (ID), and management of requests from unauthorized entities. For visibility control of IM ID, it is necessary for a user to decide whether their information (e.g., IM ID, nickname, location) should be visible to an unauthorized user. For management of requests from unauthorized entities, it is required that a user is able to choose a suitable policy to handle these requests. A user should be able to manually approve, require a precise answer to a personal question, or even block all requests. Further, a user should also have the ability to specify trusted friends, and manage a friend’s list on the IM client.

2) Blacklist management

Users should be able to manage their user-specific blacklist themselves, and all messages sent from accounts listed in their user-specific blacklist should be blocked. The user should be able to add, delete or even share their user-specific blacklist.

3) SPIM complaints

The IM client should have a function to submit complaints about accounts that send SPIM. The complained-about account may be a contact in the user's friend list, a member in an IM group, or even an unauthorized account that sends authorization requests.

4) Anti-SPIM database

- User friend list: It is required to store a list of friends approved by the user.
- User-specific blacklist: It is defined by users, which includes accounts that the user wants to block messages from.

The database located in the IM client shall be automatically uploaded to the IM server.

8 Working procedures

8.1 Working procedure of sending rate control

The threshold that defines the maximum number of messages allowed to be sent from a given IM account, within a given time period, should be set in the IM server.

The threshold should be studied or trained, using a large number of samples of user messages, using technologies such as machine learning, deep learning, etc. The threshold should be set respectively in different scenarios, including, but not limited to, the following:

– The instant messages are sent to a group, and the sender is a member of the group;

– The instant messages are sent to a group, but the sender is not a member of the group;

– The instant messages are sent to one or more of the sender's friends;

– The instant messages are sent to non-friends of the sender.

When the IM server receives messages sent by a specified account, the IM server shall implement sending rate control through the following process, as illustrated in Figure 8-1:

– Count the number of messages sent by the account within a given time period;

– Compare the number of messages sent (n) with the minimum threshold set for all scenarios. If the number (n) exceeds the minimum threshold, the IM server further determines to which scenario it belongs, and whether the number (n) exceeds the threshold of that specific scenario. If not, the IM server forwards the messages;

– If the number of messages sent (n) exceeds the specific threshold, the IM server checks to see whether the account is listed in the integrated suspicious list. If in this list, the IM server discards the messages; if not, the IM server forwards the messages but counts the number of excess times (m). If this number (m) is more than a given number (α), the IM server adds the account to the suspicious list.

The process of implementing sending rate control is illustrated in Figure 8-1:

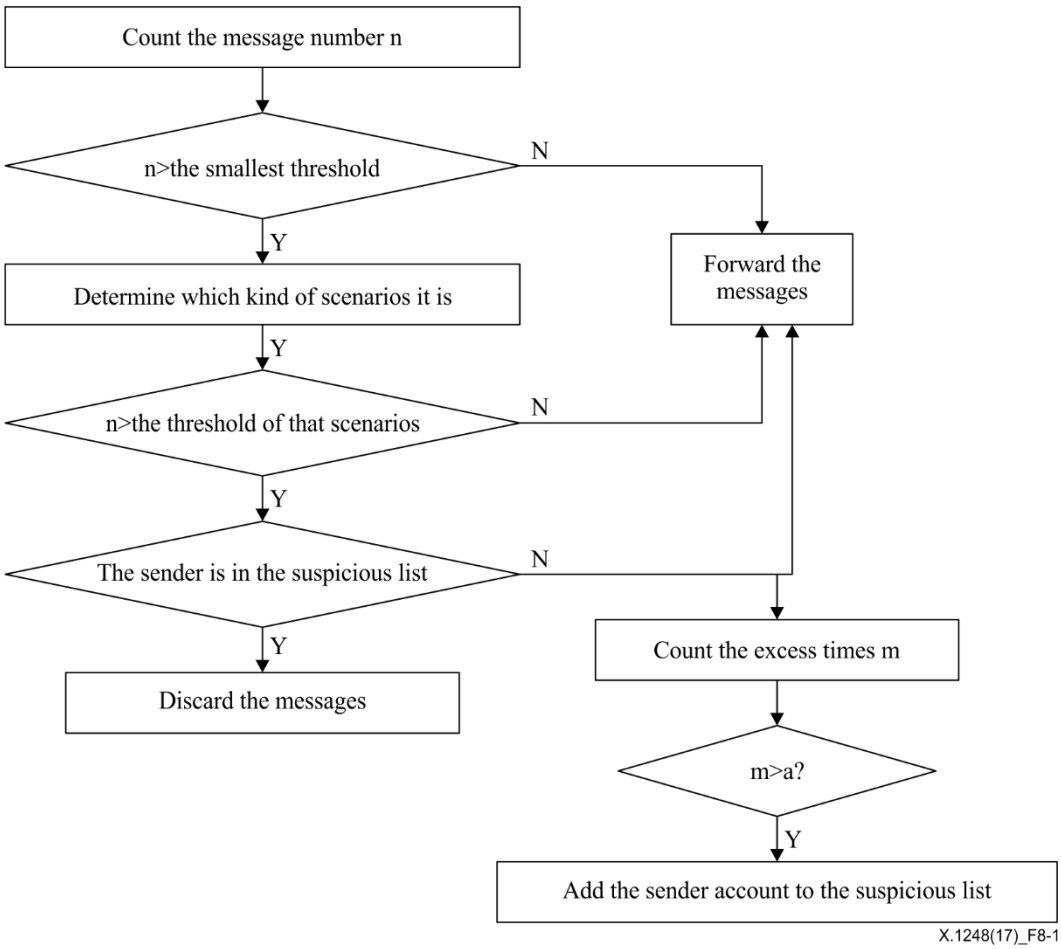

Figure 8-1 – The process of implementing sending rate control

8.2 Working procedure of blacklists

IM systems are comparatively independent; thus IM service providers are required to build their own integrated blacklists for their IM servers. Additionally, for users' benefit, it is required that user-specific blacklists are provided on the IM clients.

The interaction process of all types of blacklists in an IM system is as follows:

– The user edits their user-specific blacklist on the IM client. The IM server monitors the user-specific blacklist in real-time and updates the set of user-specific blacklists when the user-specific blacklist changes;

– The IM server tracks the number of times the same account has been added to user-specific blacklists. If the number exceeds a given threshold, the IM server adds that account to the integrated blacklist;

– The IM server will add the account referenced in a client complaint to the integrated suspicious blacklist if the account is neither in the integrated suspicious blacklist nor in the integrated blacklist. The IM server counts the number of times a complaint has been registered for the account; if the number exceeds a given threshold, the IM server adds this account to the integrated blacklist.

The process of filtering messages based on blacklists is as follows:

– When the IM server receives a message, the server checks whether the sender's account is in the integrated blacklist; if it is, the IM server discards the message;

– If the sender's account is not in the integrated blacklist, the IM server can further check whether the sender's account is in the receiver's user-specific blacklist, and if it is, the IM server discards the message. If it is not, the IM server forwards the message.

8.3 Procedures of authorization management

It is recommended that an IM client has a function to allow users to define which kind of messages can be received, and the IM server should have the ability to filter unwanted messages according to the user's definition, to prevent unauthorized senders (e.g., non-friends, non-friend members in a group, friends of other IM systems, phone contacts) from sending unwanted messages. The scenarios that authorize senders include, but are not limited to, the following five steps:

1) Set the IM client to 'only receive messages from friends'. When the IM server receives a message sent from user B to user A, the IM server shall check whether user B is in user A's friend list. If not, the server discards the message.

2) Set the IM client to 'receive messages from a group that the client has explicitly joined'. When the IM server receives a message sent from group B to user A, the server shall check whether user A is a member of group B. If not, the server discards the message. In addition, when the IM server receives an invitation sent from a member of group B to user A, it should be permitted by user A before the IM server adds user A to group B.

3) Set the IM client to 'receive messages from a member of a group that the client is a friend of'. When the IM server receives a message sent from group A's user B to user A, the server will check whether user B is in user A's friend list. If not, the server discards the message.

4) Set the IM client to 'receive messages from accounts of other IM systems or phone contacts only after having explicitly added these accounts or contacts as friends'. When the IM server receives a message sent from associated account B to user A, the server shall check whether account B is in user A's friend list. If not, the server discards the message. Additionally, when the IM server receives a request to add a friend from account B to user A's friend list, it should be permitted by user A before the server adds account B to user A's friend list.

5) Set the IM client to 'restrict establishment of a point-to-point connection only to friends'. When the IM server receives a request from user B to establish a point-to-point connection with user A, the server will check whether user B is user A's friend list. If it is, the IM server shall forward user B's request to user A, and assist user A and user B in establishing a point-to-point connection. If not, the IM server shall discard user B's request.

The relationship of user A, user B, group A, group B, account B is illustrated in Figure 8-2.

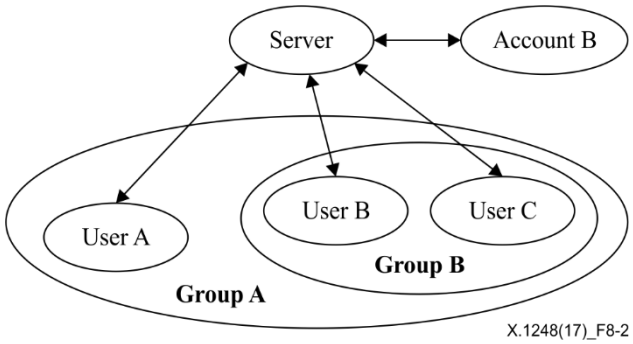

Figure 8-2 – The relationship of users and groups

8.4 Procedures of user registration management

To prevent the automatic registering of accounts, IM systems should implement one or more manual confirmation measure, such as verification code, e-mail verification, SMS verification code.

When a user submits registration information (e.g., user name, password, mobile phone number, e-mail address) on the IM client or IM user registration webpage, the IM server sends a registration confirmation back to the user, such as verification code, SMS verification code, or registration confirmation e-mail.

Once the user sends the registration confirmation back to the IM server, the IM server verifies the registration confirmation submitted by the user. If the verification is valid, the IM server returns a registration success message to the user, and saves the user's registration information to the database. If not, it returns a registration failure message.

The IM system should interface with an SMS gateway or deploying mail server, so as to achieve the function of sending an SMS verification code or registration confirmation e-mail to the user.

8.5 Procedures for SPIM complaints

Two procedures for reporting SPIM complaints should be supported as follows:

1) Complaint through the IM client. With this method, the complaint-handling process is illustrated as follows:

   IM users mark the SPIM account on the IM client after receiving the SPIM; the complaint is sent to the IM server. The IM server should have a complaint threshold predefined. Upon receiving a user's complaint, the IM server first checks if the account is already in the integrated suspicious blacklist or in the integrated blacklist. If not, the IM server adds the account to the integrated suspicious list, and counts the number of times that the account has had complaints. If this number exceeds the predefined threshold, the IM server adds the account to the integrated blacklist. If the account is already in the integrated suspicious blacklist, the IM server accumulates the number of times that the account has had complaints. If this value exceeds the predefined threshold during a given period of time, the IM server adds this account to the integrated blacklist. If the account is already in the integrated blacklist, the IM server does nothing. Messages later sent by this account should be discarded by the IM server.

2) Complaint through an external SPIM complaint-handling system. With this method, the complaint-handling process is illustrated as follows:

   IM users complain to an external SPIM complaint-handling system after receiving SPIM. The external SPIM complaint-handling system is in charge of analysing the user's complaint and deciding whether to add the account to the blacklist. The IM server interfaces with the external SPIM complaint-handling system and imports or exports the blacklist from the interface. Messages sent by accounts in the blacklist shall be discarded by the IM server.

8.6 Procedure of SPIM filtering

When an IM server receives instant messages, it carries out SPIM filtering based on the integrated blacklist and user-specific blacklist set; this process is described in clause 8.2.

If the IM sender's account is not in the integrated blacklist and user-specific blacklist set, then the IM server carries out SPIM filtering based on authorization control and analyses whether the sender has authorization to send messages to the recipient (which is set by the recipient). If not, the message is dropped. The authorization scenario is described in clause 8.3.

If it is, the IM server then carries out SPIM filtering based on the sending rate limit; this process is described in clause 8.1.

Appendix I

Roles and functions of IM system

(This appendix does not form an integral part of this Recommendation.)

The basic IM system model is shown in Figure I.1.

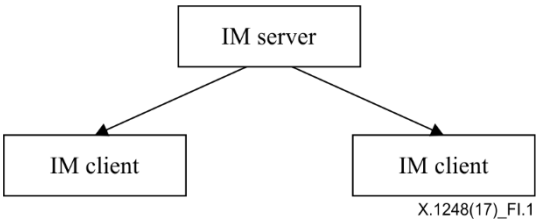

Figure I.1 – Basic IM model

The basic IM system model includes an IM server and multiple homogenous IM clients. The IM server is used to receive and forward instant messages that are sent by IM clients. The IM client has two roles: IM sender and IM receiver. The IM sender forwards instant messages to the IM server for delivery, and the IM server attempts to deliver the messages to corresponding IM receivers. If an IM sender sends SPIM, then it is considered to be a spimmer.

The functions of the IM system need to be completed by the IM server, IM clients, and the interaction between them.

The main functions of the IM server include the following:

– User management, such as user registration, user login and logout, user account edit;
– Instant message management, such as message sending, message receiving, message transmission;
– Friend management, such as friend searching, friend list managing;
– System management, such as parameter configuration, system update, system start/restart/quit.

The main functions of the IM client include the following:

– User management, such as user registration, user login and logout;
– Instant message management, such as message sending, message receiving;
– Friend management, such as friend adding, friend deleting, friend searching;
– Client management, such as parameter configuration, client update, client start/restart/quit.

Bibliography

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

[b-ITU-T X.1240] Recommendation ITU-T X.1240 (2008), *Technologies involved in countering e-mail spam*.

[b- ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-IETF RFC 2778] IETF RFC 2778 (2000), *A Model for Presence and Instant Messaging*.

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging*.

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, 2017