

I n t e r n a t i o n a l   T e l e c o m m u n i c a t i o n   U n i o n

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**X.1244**

(09/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM  
COMMUNICATIONS AND SECURITY

Telecommunication security

---

## **Overall aspects of countering spam in IP-based multimedia applications**

Recommendation ITU-T X.1244

ITU-T X-SERIES RECOMMENDATIONS  
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

|                                               |                |
|-----------------------------------------------|----------------|
| <b>PUBLIC DATA NETWORKS</b>                   |                |
| Services and facilities                       | X.1–X.19       |
| Interfaces                                    | X.20–X.49      |
| Transmission, signalling and switching        | X.50–X.89      |
| Network aspects                               | X.90–X.149     |
| Maintenance                                   | X.150–X.179    |
| Administrative arrangements                   | X.180–X.199    |
| <b>OPEN SYSTEMS INTERCONNECTION</b>           |                |
| Model and notation                            | X.200–X.209    |
| Service definitions                           | X.210–X.219    |
| Connection-mode protocol specifications       | X.220–X.229    |
| Connectionless-mode protocol specifications   | X.230–X.239    |
| PICS proformas                                | X.240–X.259    |
| Protocol Identification                       | X.260–X.269    |
| Security Protocols                            | X.270–X.279    |
| Layer Managed Objects                         | X.280–X.289    |
| Conformance testing                           | X.290–X.299    |
| <b>INTERWORKING BETWEEN NETWORKS</b>          |                |
| General                                       | X.300–X.349    |
| Satellite data transmission systems           | X.350–X.369    |
| IP-based networks                             | X.370–X.379    |
| <b>MESSAGE HANDLING SYSTEMS</b>               | X.400–X.499    |
| <b>DIRECTORY</b>                              | X.500–X.599    |
| <b>OSI NETWORKING AND SYSTEM ASPECTS</b>      |                |
| Networking                                    | X.600–X.629    |
| Efficiency                                    | X.630–X.639    |
| Quality of service                            | X.640–X.649    |
| Naming, Addressing and Registration           | X.650–X.679    |
| Abstract Syntax Notation One (ASN.1)          | X.680–X.699    |
| <b>OSI MANAGEMENT</b>                         |                |
| Systems Management framework and architecture | X.700–X.709    |
| Management Communication Service and Protocol | X.710–X.719    |
| Structure of Management Information           | X.720–X.729    |
| Management functions and ODMA functions       | X.730–X.799    |
| <b>SECURITY</b>                               | X.800–X.849    |
| <b>OSI APPLICATIONS</b>                       |                |
| Commitment, Concurrency and Recovery          | X.850–X.859    |
| Transaction processing                        | X.860–X.879    |
| Remote operations                             | X.880–X.889    |
| Generic applications of ASN.1                 | X.890–X.899    |
| <b>OPEN DISTRIBUTED PROCESSING</b>            | X.900–X.999    |
| <b>TELECOMMUNICATION SECURITY</b>             | <b>X.1000–</b> |

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

# **Recommendation ITU-T X.1244**

## **Overall aspects of countering spam in IP-based multimedia applications**

### **Summary**

Recommendation ITU-T X.1244 specifies the basic concepts, characteristics, and technical issues related to countering spam in IP multimedia applications such as IP telephony, instant messaging, etc. The various types of IP multimedia application spam are categorized, and each categorized group is described according to its characteristics. This Recommendation describes various spam security threats that can cause IP multimedia application spam. There are various techniques developed to control the e-mail spam which has become a social problem. Some of those techniques can be used in countering IP multimedia application spam. This Recommendation analyses the conventional spam countering mechanisms and discusses their applicability to countering IP multimedia application spam. This Recommendation concludes by mentioning various aspects that should be considered in countering IP multimedia application spam.

### **Source**

Recommendation ITU-T X.1244 was approved on 19 September 2008 by ITU-T Study Group 17 (2005-2008) under the WTSA Resolution 1 procedure.

### **Keywords**

Instant messaging spam, IP multimedia application spam, spam, voice over IP spam.

## 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 2009

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

# CONTENTS

## Page

|      |                                                                                             |    |
|------|---------------------------------------------------------------------------------------------|----|
| 1    | Scope .....                                                                                 | 1  |
| 2    | References.....                                                                             | 1  |
| 3    | Definitions .....                                                                           | 1  |
| 3.1  | Terms defined elsewhere .....                                                               | 1  |
| 3.2  | Terms defined in this Recommendation.....                                                   | 2  |
| 4    | Abbreviations and acronyms .....                                                            | 3  |
| 5    | Conventions .....                                                                           | 4  |
| 6    | Concept and typical types of IP multimedia spam .....                                       | 4  |
| 6.1  | VoIP spam .....                                                                             | 4  |
| 6.2  | IP multimedia message spam .....                                                            | 5  |
| 6.3  | Instant messaging spam.....                                                                 | 5  |
| 6.4  | Chat spam .....                                                                             | 5  |
| 6.5  | Multimodal spam.....                                                                        | 6  |
| 6.6  | Spam over P2P based file sharing service .....                                              | 6  |
| 6.7  | Website spam.....                                                                           | 6  |
| 7    | Classification of IP multimedia spam.....                                                   | 6  |
| 7.1  | Real-time voice spam .....                                                                  | 7  |
| 7.2  | Real-time text spam.....                                                                    | 8  |
| 7.3  | Real-time video spam .....                                                                  | 8  |
| 7.4  | Non real-time voice spam.....                                                               | 8  |
| 7.5  | Non real-time text spam .....                                                               | 9  |
| 7.6  | Non real-time video spam .....                                                              | 9  |
| 8    | Technical issue for countering IP multimedia spam .....                                     | 9  |
| 8.1  | Creation and delivery of spam.....                                                          | 10 |
| 8.2  | Detection and filtering of spam .....                                                       | 11 |
| 8.3  | Action for the received spam.....                                                           | 12 |
| 9    | Security threats related to spam.....                                                       | 12 |
| 9.1  | Security threats related to spam.....                                                       | 12 |
| 9.2  | Classification of spam security threats .....                                               | 14 |
| 9.3  | Countermeasures .....                                                                       | 14 |
| 10   | Applicability of well-known countering spam mechanisms for IP multimedia applications ..... | 15 |
| 10.1 | Identification filtering.....                                                               | 15 |
| 10.2 | Address masking .....                                                                       | 18 |
| 10.3 | Human interactive proof.....                                                                | 18 |
| 10.4 | Content filtering.....                                                                      | 19 |
| 10.5 | Authentication by key exchange .....                                                        | 19 |
| 10.6 | Network-based spam filtering .....                                                          | 20 |

|                                                                      | <b>Page</b> |
|----------------------------------------------------------------------|-------------|
| 10.7 Online stamp.....                                               | 21          |
| 10.8 Authorization-based spam filtering .....                        | 21          |
| 10.9 Legal action and regulations.....                               | 22          |
| 11 Considerations in countering IP multimedia application spam ..... | 23          |
| 11.1 Service user (service subscriber).....                          | 23          |
| 11.2 Service provider.....                                           | 23          |
| 11.3 Network operator.....                                           | 24          |
| 11.4 Public organization.....                                        | 25          |
| 11.5 Other considerations .....                                      | 25          |
| Bibliography.....                                                    | 26          |

## Introduction

Spam has been a social problem in the network e-mail system. Various solutions have been developed and deployed to resolve this problem, but none of them have actually solved the spam problem. The IP multimedia application consists of various types of services, such as IP telephony, instant messaging, etc. These IP multimedia services are becoming a new target for the sender of spam, since it is technically a simpler and economically cheaper approach for spamming. IP multimedia application spam must be dealt with before it becomes a public problem.

This Recommendation describes the concept and characteristics of various types of spam that can occur in IP multimedia applications. It discusses some issues on technical and security viewpoints for countering IP multimedia application spam, thus provides some consideration aspects by several participating members in providing IP multimedia service such as service providers, service users, etc. in countering IP multimedia application spam.

Rec. ITU-T X.1244 (09/2008)

.....

# Recommendation ITU-T X.1244

## Overall aspects of countering spam in IP-based multimedia applications

### 1 Scope

This Recommendation provides an overview of IP multimedia spam, with a focus on the following issues:

- Concept and characteristics of IP multimedia spam
- Technical issues related to IP multimedia spam
- Security threats related to spam
- Spam countering methods and their applicability to counter IP multimedia spam
- Various aspects that should be considered for countering spam in IP-based multimedia applications

NOTE – The use of the term "identity" in this Recommendation does not indicate its absolute meaning. In particular, it does not constitute any positive validation.

### 2 References

None.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 access control list (ACL)** [b-ITU-T X.741]: The access control list attribute is used to contain identities of initiators that are either specifically granted access to management information or specifically denied access to management information.

**3.1.2 certification authority (CA)** [b-ITU-T X.509]: An authority trusted by one or more users to create and assign public-key certificates. Optionally, the certification authority may create the users' keys.

**3.1.3 conference** [b-ITU-T T.124]: A number of nodes that are joined together and that are capable of exchanging audiographic and audiovisual information across various telecommunication networks.

**3.1.4 DomainKeys identified mail (DKIM)** [b-IETF RFC 4871]: A mechanism by which e-mail messages can be cryptographically signed, permitting a signing domain to claim responsibility for the introduction of a message into the mail stream. Message recipients can verify the signature by querying the signer's domain directly to retrieve the appropriate public key, and thereby confirm that the message was attested to by a party in possession of the private key for the signing domain.

**3.1.5 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.

**3.1.6 peer-to-peer (P2P) relationship** [b-ITU-T T.180]: In a peer-to-peer relationship, the users may negotiate the characteristics of their interaction and, afterwards, communicate obeying the rules they have negotiated; both users (an entity and its peer entity) have potentially equal rights. [b-IETF RFC 4981] indicates that P2P networks are those that exhibit three characteristics: self-organization, symmetric communication, and distributed control.

**3.1.7 pretty good privacy (PGP)** [b-IETF RFC 1991]: PGP uses a combination of public key and conventional encryption to provide security services for electronic mail messages and data files. These services include confidentiality and digital signature. PGP was created by Philip Zimmermann and first released, in Version 1.0, in 1991. Subsequent versions, e.g., open PGP that is described in [b-IETF RFC 4880], have been designed and implemented by an all-volunteer collaborative effort under the design guidance of Philip Zimmermann. *PGP and Pretty Good Privacy are trademarks of Philip Zimmermann.*

**3.1.8 public key infrastructure (PKI)** [b-ITU-T X.509]: The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.

**3.1.9 transport layer security (TLS)** [b-ITU-T Q.814]: The TLS protocol optionally provides communications privacy. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and intrusion. The TLS protocol also provides strong peer authentication and data flow integrity.

## **3.2 Terms defined in this Recommendation**

This Recommendation defines the following terms:

**3.2.1 bait spam:** Its name derived playfully from the analogy to fishing (and phishing (see clause 3.2.10)), bait spam is a variety of spam which includes an element, e.g., an e-mail subject or embedded link, to lure users. The lured user is attacked by the bait spam.

**3.2.2 blog:** A contraction of "web log"; a blog is an online, possibly multimedia, list of its owner's personal interests that is available for general public to view and, sometimes, to enhance.

**3.2.3 bot:** Bot is a contraction of "robot", which is a program that operates as an agent for a user or another program to simulate a human activity.

**3.2.4 DNS cache poisoning:** DNS cache poisoning is a technique that tricks a domain name system server (DNS server) into believing the DNS address of a certain server has been changed when, in reality, it has not. Once the DNS server has been poisoned, this information is generally cached for a certain period of time, spreading the effect of the attack to the users of the server.

**3.2.5 IP multimedia message:** IP multimedia message is a text, voice, or video message that is delivered and stored in an IP multimedia terminal or server for the recipient to check afterward. It is similar to voice mail in telephony service, but serviced in IP multimedia service.

**3.2.6 IP multimedia spam:** Unsolicited messages or calls through IP multimedia applications. To distinguish this from traditional e-mail spam, IP multimedia spam denotes spam on newly emerging telecommunication methods over IP, such as instant messaging (IM), presence, or voice over IP (VoIP) services.

**3.2.7 modality:** In general usage, this term refers to the forms, protocols, or conditions that surround formal communications. In the context of this Recommendation, it refers to the information encoding(s) containing information perceptible for a human being. Examples of modality include textual, graphical, audio, video or haptical data used in human-computer interfaces. Multimodal information can originate from, or be targeted to, multimodal-devices. Examples of human-computer interfaces include microphones for voice (sound) input, pens for haptic input, keyboards for textual input, mice for motion input, speakers for synthesized voice output, screens for graphic/text output, vibrating devices for haptic feedback, and Braille-writing devices for people with visual disabilities.

**3.2.8 multimodal message:** This is a multimedia message that contains differently encoded information for interaction via multiple modalities. For example, a MMS (multimedia messaging service) message may convey text, graphic and audio modalities. A web-page may also contain multimedia modal content such as text and video. Similarly, an e-mail may contain a graphic

attachment together with text. Multimodality enables the user to select a preferred modality due to environment, convenience or content.

**3.2.9 online game:** Real-time game that is played over the networks.

**3.2.10 phishing:** An attempt to acquire criminally and fraudulently sensitive information, such as usernames, passwords and financial account details, by masquerading as a trustworthy entity in an electronic communication.

**3.2.11 session hijacking:** A mechanism of stealing a valid user session to gain unauthorized access to information or services.

**3.2.12 spam over instant messaging (SPIM):** A spam targeting users of instant messaging service.

**3.2.13 spam over Internet telephony (SPIT):** Spam targeting users of Internet telephony service

**3.2.14 spammer:** Sender of spam.

**3.2.15 spamming:** A chain of activities carried out by spammers to send spam, such as collection of target lists, creation of spam, delivery of spam, etc.

**3.2.16 spimmer:** Sender of SPIM.

**3.2.17 spitter:** Sender of SPIT.

**3.2.18 user created content (UCC):** UCC is any form of content such as video, blog, images, audio, etc. that was created by end-users (average public) to be available for general public.

**3.2.19 user generated content (UGC):** UGC is equivalent to UCC.

**3.2.20 vishing:** An illegal act of gaining access to private personal and financial information through the voice over IP (VoIP) service. The term vishing is a contraction of "voice phishing".

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

|       |                                                    |
|-------|----------------------------------------------------|
| ACL   | Access Control List                                |
| APEC  | Asia-Pacific Economic Cooperation                  |
| ARP   | Address Resolution Protocol                        |
| ASCII | American Standard Code for Information Interchange |
| CA    | Certificate Authority                              |
| DB    | Database                                           |
| DKIM  | DomainKeys Identified Mail                         |
| HTTP  | HyperText Transfer Protocol                        |
| IM    | Instant Messaging                                  |
| IP    | Internet Protocol                                  |
| IPTV  | Internet Protocol Television                       |
| IPv4  | Internet Protocol version 4                        |
| IPv6  | Internet Protocol version 6                        |
| IRC   | Internet Relay Chat                                |
| ISP   | Internet Service Provider                          |