International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1240
(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Technologies involved in countering e-mail spam

Recommendation ITU-T X.1240

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
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
OPEN SYSTEMS INTERCONNECTION	
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
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
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
OSI MANAGEMENT	
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
SECURITY	X.800–X.849
OSI APPLICATIONS	
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
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

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

Recommendation ITU-T X.1240

Technologies involved in countering e-mail spam

Summary

Recommendation ITU-T X.1240 specifies basic concepts, characteristics and effects of e-mail spam, and technologies involved in countering e-mail spam. It also introduces the current technical solutions and related activities from various standards development organizations and relevant organizations on countering e-mail spam. It provides guidelines and information to users who want to develop technical solutions on countering e-mail spam. This Recommendation will be used as a basis for further development of technical Recommendations on countering e-mail spam.

Source

Recommendation ITU-T X.1240 was approved on 18 April 2008 by ITU-T Study Group 17 (2005-2008) under the WTSA Resolution 1 procedure.

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/.

CONTENTS

Introduction

As requested by WTSA-2004 Resolution 52 'Countering spam by technical means', standardization work was undertaken to develop ITU-T Recommendations that help countering spam by technical means. This Recommendation is one of a series of ITU-T Recommendations for countering e-mail spam which consist of guidelines, requirements, a technical framework and technical strategies. Other ITU-T Recommendations on countering spam for IP multimedia applications such as IP telephony, instant messaging and conference will be developed as separate documents.

Recommendation ITU-T X.1240

Technologies involved in countering e-mail spam

1 Scope

This Recommendation specifies the technologies involved in countering e-mail spam. It introduces the current technical solutions and related activities from various standards development organizations and relevant organizations for countering e-mail spam. The purpose of this Recommendation is to provide useful information to users who want to develop technical solutions for countering e-mail spam. This Recommendation will be used as a basis for further development of technical Recommendations on countering e-mail spam.

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

This Recommendation defines the following terms:

3.1 **phisher**: An entity or a person launching phishing attacks.

3.2 **phishing**: Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using trojan keylogger spyware.

3.3 **spam**: 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.

3.4 **spammer**: An entity or a person creating and sending spam.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
DKIM	DomainKeys Identified Mail
CSV	Certified Server Validation
DNS	Domain Name System
DSN	Delivery Status Notification

HTML	HyperText Markup Language
IM	Instant Messaging
ISP	Internet Service Provider
META	Message Enhancements for Transmission Authorization
MMS	Multimedia Messaging Service
MTA	Mail Transfer Agent
OECD	Organization for Economic Co-Operation and Development
OPES	Open Pluggable Edge Services
PGP	Pretty Good Privacy
PTR	Pointer Record
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPF	Sender Policy Framework
TEOS	Trusted Email Open Standard

5 Conventions

None.

6 Introduction to countering e-mail spam

6.1 Concept and Characteristics of spam

Although there is no universally agreed definition of spam, the term is commonly used to describe unsolicited electronic communications over e-mail, mobile messaging (SMS, MMS) and instant messaging services, usually with the objective of marketing commercial products or services.

While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media, e.g., mobile phone messaging spam, IP-based telephony spam, instant messaging spam, Usenet newsgroup spam, web search engine spam and blog spam. The content of the spam messages ranges from advertisement of goods to offensive pornographic material. E-mail spam has various kinds of harmful effects to e-mail service users and internet service providers:

– Spam recipients and ISPs spend a lot of time, money and effort to identify, delete and filter spam.
– E-mail spam may include deceptive contents alluring to spam recipients, or adult content inappropriate for children.
– E-mail service users and ISPs suffer from the waste of network resources and storage.
– Spread of virus and spyware can be a threat to the network security.
– E-mail spam decreases the visibility of normal and important e-mails.

A recent and growing phenomenon is the use of spam to support fraudulent and criminal activities, including attempts to capture financial information (e.g., account numbers and passwords) by masquerading messages as originating from trusted companies ("brand-spoofing" or "phishing"), as well as a vehicle to spread viruses and worms.

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through domain name system (DNS) hijacking or poisoning.

Spammers have proven themselves to be highly creative in avoiding detection, including falsification of origin of e-mail and randomization of content to bypass spam filters. The scale of the problem has grown to such an extent that anti-spam laws are being rapidly enacted in a number of countries, although different national approaches and remedies are used. At the same time, there is increasing recognition that countering spam is an issue requiring international coordination and cooperation.

6.2 Approaches to countering e-mail spam

Since e-mail spam does great damage to e-mail service users, ISPs and network operators, technologies have been developed and regulations have been adopted in many countries to help counter spam. However, it is difficult to counter spam effectively through a single countering measure such as filtering or legal punishment since countering spam is not a simple problem. For that reason, various methods should be applied simultaneously to counter spam effectively:

– Regulation: Anti-spam regulations should be adopted to facilitate the appropriate response of service users for e-mail spam and to increase the effect of anti-spam technologies such as filtering. In addition, regulation can help protect service users and ISPs from illegal spam.

– Technology: Anti-spam technology development is essential for countering large quantities of e-mail spam effectively. It is required to develop various technologies to prevent sending spam, and to identity and filter spam effectively.

– Industrial action: Various kinds of anti-spam technologies, including blacklist or whitelist and filtering functions, are appropriate to be developed and installed by industry participants such as ISPs or network operators. It is also possible for ISPs to adopt policies for countering e-mail spam.

– International cooperation: International cooperation is required, since telecommunication networks are borderless, and the generation and effect of spam are not domestic. International cooperation is also useful for information sharing about effective regulation adoption, anti-spam technology development, and education of service users and providers.

– Education: To minimize the damage caused by e-mail spam, education of service users and ISPs is important. The education is expected to help e-mail users take appropriate actions for e-mail spam, and ISPs to adopt anti-spam policies and technologies.

Among various anti-spam measures introduced above, this Recommendation focuses on technical means for countering spam such as development and application of anti-spam technologies.

7 Anti-spam technologies

The report of the OECD Task Force on Spam [b-OECD TF] provides several elements for countering e-mail spam including regulatory approaches, enforcement concerns and technical solutions. This Recommendation includes a reference to a part of the report (Element IV – Anti-spam technologies) in this clause. Consideration is required because the anti-spam toolkit was published in May 2006 and has not been updated since.

This clause contains discussions of the various anti-spam technologies and their capabilities presently available, as well as of the methods to be employed when spam is received. Any attempt to combat spam effectively needs to involve the sensible administration of a number of these technologies in concert. None of the methods will be entirely successful in isolation. When a number of anti-spam technologies are effectively used in collaboration with one another, the effect can drastically reduce the level of spam impacting a system.

7.1 Overview

Spam presents complex technical challenges, and therefore solutions to eliminate it need to be supported by appropriate technical measures. While government action and legislation are helpful, they are insufficient to meet the challenges posed by spam. In fact, spam is primarily a technological problem resulting from a flaw in the SMTP protocol. The technical nature of the problem makes it particularly difficult for enforcers to identify spammers, and therefore to punish them.

Notwithstanding varying definitions of spam, there are both technologies and techniques that can be used to help control the problem of unwanted e-mails. This clause is meant to provide a neutral overview of the various types of technological tools and methods as well as factors to consider prior to their implementation. It refers specifically to tools as opposed to solutions. While technology is designed to address many of the problems created by spam, and may in fact "solve" some of the specific issues related to spam, an overall solution to spam can only be achieved through a multi-faceted approach that includes technology, policy (including regulation where appropriate), practice and education.

Anti-spam tools operate at many levels – point of origination, in the backbone, at the gateway and on the recipient computer – and may be used alone or in combination. Updated information and resources are available on the toolkit website at www.oecd-antispam.org.

This clause is addressed in particular to mail server managers, in order to provide them with an insight into the strong and weak points of each filtering technique, to enable them to choose software according to their e-mail policy and needs, depending upon their planned architecture. The focus of this clause is on practices for incoming mail, although practices aimed at reducing outgoing spam would also be useful. In addition to operators of receiving servers, operators of sending servers have a role to play. Operators of sending servers can employ outbound rate limiting and port 25 blocking, and employ other measures to reduce the amount of spam being sent from their servers.

Tools that deal with spam need to focus on both the mail and on the behaviour surrounding the mail. In light of these multiple factors, many instruments and methods are based on sets of rules or assumptions that work alone or in combination to identify suspect e-mails. Over time, spam has grown in scope to include more viruses and malware. This requires defensive technology to go beyond text-based tools to tools that analyse behavioural and contextual factors in determining whether to accept or reject specific mail or even attempted connections. Considering the increased security threat presented by spam, we expect that anti-spam technologies will either contain more, or need to work in conjunction with, advanced security and authentication technologies.

7.2 The importance of tool/technology context

Some of the tools/technologies considered in this clause are specifically designed to be implemented at the entrance to the e-mail platform, whereas others can be more usefully deployed after the receipt of messages but prior to delivery to the end user. It is important to note that some tools also reside on the recipient's computer. At each stage of filter application, the aim of implementing a rule may be to refuse or reject the electronic message, or simply to mark it or deliver it to the end user's spam box.

The relevance and usefulness of each rule can therefore only be judged in terms of the precise context in which it is applied, the level at which it is applied in the message distribution process, and what finally happens to the communications.

7.3 Combining tests

Technology should be the backbone of any approach that aims to defeat spam. One should be aware that none of the technologies discussed in the following clauses will act as a "silver bullet" or one-stop solution to the problems created by spam. Rather, all of the technologies are complementary and will be most effective when implemented in conjunction with each other. The integration of a number of technologies is necessary to reduce the harmful impact of spam on a system.

Tests should not necessarily be used in "all or nothing" mode. On the contrary, it is preferable to combine tests to maximize the number of spam e-mails intercepted while minimizing the number of legitimate e-mails inadvertently intercepted or refused.

– All or nothing refusal – this is one possible response from services using a blacklist. Any message that fails the test is refused. The occurrence of the error does depend, however, on where the rule is located in the distribution process.

– Access privilege – this is one possible response from servers using a whitelist. Any message that passes the test is accepted. There is no risk of a legitimate message being rejected, but there may be false negatives. For example, a domain whitelist is of no real interest if the sender's domain is not authenticated (with sender policy framework or domainkeys identified mail, DKIM).

– Many spam messages or worms claim to originate from recognized consumer brands in the hope of gaining access privilege.

– Scoring – this is how programs combine their tests. Avoiding the inconveniences of "all or nothing", scoring is highly recommended. However, it is costly in terms of machine resources and the continued requirement of updating scoring factors to maximize hits while minimizing false positives.

The conventional method is to run several "all or nothing" tests and then score the messages that have been allowed in.

7.4 Types of anti-spam technologies

7.4.1 Authentication of electronic mail

Mail authentication methods fall into the category of rules, which, although they help in the fight against spam, do not constitute specific anti-spam technologies.

An analogy may help to make this clear. Identity cards are not a trust marker in that perpetrators may also have an identity card. The requirement for transparency, however, will be of greater benefit to legitimate senders than to spammers.

7.4.2 SPF and/or Sender-ID

A major force behind the proliferation of spam is the ability of spammers to hide the true return address of their messages. The architecture of electronic mail does not imply a prior contact between the sender and the recipient. Therefore, it is not possible to rely on systematic authentication. The problem is of growing concern because forged addresses have been used in phishing scams that lure message recipients into disclosing credit card numbers and other personal information.

The application of this technology is still emerging and therefore lacks standardization, but authentication works by flagging e-mail messages whose true senders cannot be verified. A receiving server can choose to block unauthenticated messages, but the technology does not require it to do so. The technology merely flags the message. The key advantage of domain – level authentication is that it will significantly reduce false positives and permit more reliable filtering based on reputation. The increased costs for senders are offset by guaranteed message delivery if senders are authenticated and are using the system legitimately, or by risk of legal liability for brand misuse. The specifics of the verification process vary with the model chosen, and several server authentication models currently exist. Two of the most prevalent are sender policy framework (SPF) and Sender-ID.

These two techniques can be discussed together because they share several common features. The question of which one to choose, however, is less straightforward.

SPF and Sender-ID can be used to test whether an e-mail server is authorized to send an e-mail on behalf of a given domain. This is done by publishing a record in the Domain Name System (DNS), which lists the authorized e-mail servers for a domain. The two techniques primarily differ in the choice of the identity tested. SPF tests the envelope's MAIL FROM [b-IETF RFC 2821], while sender-ID tests the headers [b-IETF RFC 2822].

Server administrators take two types of action – they publish SPF records in the DNS and they test them on entry. According to a recent report [B-Lyris], the use of an improper SPF record now dramatically decreases the chances that a message will be delivered.

The authentication of electronic mail by checking the IP addresses of the sender's server will help to reduce and manage spam in the future. This will probably call for the creation of services above authentication, for example private whitelists, reputation services, and accreditation services.

7.4.3 DKIM and/or META

DKIM and message enhancements for transmission authorization (META) are used to authenticate the sender domain by means of a cryptographic signature automatically added by the e-mail server. The authentication of electronic mail by cryptographic signature of the message should help to reduce and manage spam in the future.

DKIM is the most publicized of these models. The model works by requiring a digital signature, or private key, on all outbound messages. The incoming messages are authenticated at the domain and mail server levels by ensuring that the private key matches the public key already on file. This method ensures that the message could only have come from the originating ISP. DKIM benefits the sender domain by ensuring delivery to ISPs that run the DKIM algorithm. DKIM was recently approved as an RFC by the Internet Engineering Task Force, thereby making it the IETF standard.

7.5 Existence of the sender's domain and eliciting a response

Many spammers send mail with a non-existent sender's address. A rule can be used to refuse these messages, such as the Postfix directive reject_unknown_sender_domain or the j-chkmail directive BadMX. Another possibility is to verify the validity of the record for the incoming server (MX) for the domain given in the "from" field of the message. Some spammers set up a dummy MX record to avoid angry replies of protest (for instance, the MX goes to 127.0.0.1, which means the local sender).

These rules call for a small amount of DNS traffic, which probably would have occurred anyway during the reply, and they can also reject a certain amount of spam.

7.6 Existence of a pointer record (PTR)

A PTR of the DNS can be used to translate the IP address of the sender's server into a name, although without necessarily checking that this name is consistent with the sender's domain.

The addition of such records is not always under the control of the sender's domain (if there is no addr.arpa delegation by the IP, for example), which, even if it is legitimate, may be unable to meet the obligation. These records can be used to determine the source of an e-mail message and whether or to what extent it can be trusted. They can also be used to determine whether a mail originates from a residential IP address or to redeliver an error message to the right server.

7.7 Blacklists/whitelists

Traditional filtering as well as tracking complaints across user communities can ultimately lead to whitelists of acceptable senders and blacklists of suspected spammers. The whitelist/blacklist approach is often too drastic a solution to be acceptable by most users. Whitelists are time-consuming to create and will require continual updating. Blacklists require similar monitoring. All lists need mechanisms and procedures for updating to address false positives and fraudulent complaints to a listing. Spoofing and open relays can also create issues related to the appearance that mail has originated from a source.

Blacklists are based on the principle of listing sources of spam. This list can include the names of machines, IP addresses or electronic addresses. It can be implemented by an entity for shared use, or introduced and maintained by the server using it for its own requirements.

With current mail transporter agents (MTAs), this test can be carried out in the SMTP session and therefore result in rejection even before the message is sent. Some lists contain open relays that do not send spam alone. Their open relay configuration can be treated as illegitimate behaviour by the platforms to which messages are sent.

The quality of blacklists varies enormously depending on the professionalism of the compiler. Many lists are poorly managed, abandoned or of dubious integrity: names can be added quickly, the applied criteria may be unclear and the removal from the list may be virtually impossible or be operated only on a payment basis. This problem is mainly due to the absence of a code of conduct or any kind of regulation to discipline and limit the functioning of blacklists. If this solution is to be used in the future, a cooperative effort to establish a list of good practices, clearly establishing cases in which addresses can be blacklisted and the conditions under which they will be removed from the lists, is necessary.

Blacklists will inevitably contain inaccuracies that will prevent some legitimate messages from getting through to the consumer. This problem, known as the false positive problem, has led to legal disputes when legitimate senders believed they were erroneously placed on an ISP's blacklist. Further, the false positive problem for individual users can result in a serious drawback of relying solely on traditional filtering technology to stop spam. However, false positives can result from most anti-spam measures. Domain level authentication should limit false positives.

Although their utilization raises many concerns, blacklists are a quick solution to refuse a connection to machines whose behaviour endangers the security or quality of services of the platform to which mail is sent, or to reject messages from certain senders.

7.8 Address of the sending server treated as either "dynamic" or "residential"

This is a particular form of blacklist in which the criterion for addition to the list is the fact that the IP address being blocked corresponds to the machine of an individual subscriber to an ISP and not to the mail server of an organization. The idea is that an ordinary subscriber does not send mail directly in SMTP, but passes through the PTA of his provider. This typically means the machine being blocked is directly sending spam messages from a spammer, or more commonly that the messages are being sent without the owner's knowledge (i.e., the machine has been compromized and turned into a "zombie" in order to send the messages).

The lists of such addresses are not always reliable since most of them have been compiled using heuristics, such as the presence of "adsl" in the name of the machine. Managing such lists is also resource-intensive.

In contrast, some of these lists, notably those compiled by the server using them, can be used to distinguish between servers authorized for a domain and the residential lists. Moreover, some domains publish the ranges of residential addresses for their domain.

This test can be seen as discriminating between "pure consumers" and "providers". The latter consider legitimate the policy by which the owner of a domain refuses to connect his machines to residential addresses, as these are currently the main source of spam. Consumers however argue that spam exists and the freedom to use e-mail must be protected.

7.9 Filtering

Filtering is the most common technical anti-spam technology. The main benefits of filters are the ease of implementation and the flexibility that users have in deciding which messages should be treated as spam. Heuristic filters require that users specify criteria, such as keywords or a sender's address that will prompt the filter to block certain messages from reaching the consumer's inbox. Spammers who deliberately misspell words or spell them in a different language easily outsmart the keyword approach. Bayesian filters are based on experience. They create statistics about the messages in a recognition table for future reference for individual users to distinguish between spam and legitimate mails. The filter then lets through only messages that resemble the user's previous legitimate mail. A study conducted by the U.S. Federal Trade Commission in 2005 [b-FTC] showed that filters can block 90% of spam.

7.9.1 Heuristic filters

These filters are based on the principle of testing for the presence in the message of certain typical features of spam, such as the exclusive use of HTML or the type of customer to whom the mail is sent. The test is weighted through a learning process based on a set of known spam mails and a set of mails known to be legitimate (the scores are therefore not calculated by a human in order to reduce subjectivity).

These filters carry the risk that a message using spammer techniques – spectacular messages in HTML, for example – will be classified as spam. Furthermore, it should be noted that the filters use large amounts of machine resources.

These filters can detect a high proportion of spam mail and they do not need to be taught or configured. However, since they use a large number of tests, it is best to be aware that it is possible to change which tests are run and the scores used to classify messages as spam.

7.9.2 Keyword filters

These are binary filters that search for a keyword ("Viagra," etc.). The risk of false positives is very high and the ability to avoid these by spacing, alternate characters and misspelling is also substantial.

7.9.3 Summary or hash value filters

Hash value filters construct a hash value of the message submitted to them and indicate whether it has already been identified as spam. There are many false negatives because a number of types of spam mail are not identified even when the server scans them with hash value filters. Furthermore, the message sometimes varies sufficiently for it to generate a different hash value. One solution to this problem is to delay the mail (as greylisting does). They generate few false positives.

7.9.4 Bayesian filters

The principle on which the Bayesian filter works is to prime its engine by examining a set of known spam e-mails and a set of e-mails known to be legitimate then, after teaching itself the vocabulary used by spammers from this known list, it will use Bayesian probabilities to calculate whether a message is spam. In the case of a group filter, the learning is usually conducted by the system administrator.

Being based on the concept of spam vocabulary, these filters can pose problems when used on a shared basis. In a small-scale and highly uniform environment (for example a firm or a university department in which everyone works in the same domain with similar vocabularies), this may be acceptable. However, this would undoubtedly not be the case for a major e-mail provider and particularly a public provider unless the group base offers each individual user the possibility of customising the filter for his/her own mailbox. The problem is that what is acceptable vocabulary to some users may trigger the filter if it has been deemed by the group to be spammer vocabulary.

Despite potential issues at the group level, these filters are highly effective when used by individual users and are one of the few solutions which, when used alone, can filter out almost all spam mail after suitable training.

7.9.5 Behavioural filters

This type of filter examines the behaviour of the remote server, such as the number of mails sent by unit of time. Rate limiting is one example of this type of filtering. The idea is that ordinary mails are only sent individually or in very small numbers and spam mails are sent in very large batches.

This type of filter is extremely delicate because typically there is no way to distinguish between a spammer and a legitimate distribution list server, such as a newsgroup.

According to some experts, it is nonetheless legitimate for a platform to refuse certain volumes of mail, primarily due to its size or its mission to ensure the security of its networks. It would also seem legitimate to ask bulk mail senders to respect the resources of the remote platform by bearing the cost of distributing their messages without trying to send them too quickly in order to free themselves from the costs inherent in using e-mail as a channel of communication.

7.10 HELO/CSV

A sending computer identifies itself by name to a receiving computer at the beginning of each SMTP transaction, by means of the SMTP "EHLO", or "HELO", command.

Certified server validation (CSV) is a service that provides a mechanism for a mail-receiving server to assess a mail-sending server. It builds upon the existing practice of service providers that accredits the networks from which sending systems are connecting.

HELO tests check that the remote MTA is properly configured, but these tests do not indicate whether it is a spammer or not. CSV tests add a probability test on the name: does it really correspond to a domain? Unlike SPF or DKIM, CSV does not authenticate the domain sending the message but rather the domain of the e-mail server (which may be different, for example, in the case of a provider serving a large number of customers).

Configuration directives – for example the Postfix directive reject_invalid_hostname – test the name announced by the server. Using conventional HELO tests, results in a very high number of legitimate messages being rejected. However, at the moment, few sites know how to modify HELO to make it work properly. This is probably going to change in the future since a growing number of sites will test HELO, thus creating an incentive to improve it.

7.11 Greylisting

This is the deliberate sending of an SMTP 4xx error code (a temporary error as opposed to a 5xx definitive error, see [b-IETF RFC 2821]) when encountering a new sender. The latter, if it is a normal MTA, will try again later (usually 15 minutes later) and its message will then be accepted. Most spam software programs do not make multiple send attempts. This technique is highly effective and blocks all spam mails that are not sent through an open relay or by the MTA of a provider. It prevents receipt of certain messages from poorly configured servers and lends itself particularly well to being used in conjunction with a whitelist.

7.12 Tokens/passwords

The aim of these techniques is to include a password in the address to which the e-mail is sent or to use a challenge/response system such as the Turing test. The spammer's software will not know this password and will be unable to pass the test.

These techniques have no false negatives, unless spammers decide to employ thousands of people at very low labour costs to do the work.

A certain number of legitimate users will refuse to or will be unable to pass the test. There will therefore be many false positives. These techniques are only of interest to highly popular recipients who already receive vast amounts of bulk mail, including legitimate mail, or to any recipient who wants to reduce the number of messages received, which falls within the scope of freedom of communication. It is necessary to be aware that not every sender will accept the test imposed. Educating users about the merits of this technology and taking the test may help reduce the non-acceptance rate.

7.13 Various techniques

This clause covers various techniques mostly experimental or insufficiently tested.

7.13.1 Envelope tests (bounce address tag validation (BATV) and signed envelope sender (SES))

These techniques are recent developments and insufficiently deployed to be taken into consideration.

7.13.2 Certification of Bulk Mails – Sender reputation

Although effective sender authentication will give ISPs a much more straightforward task when dealing with spam, authentication is only a preliminary step toward eliminating spam. Once the sender can be identified, factors such as reputation and accreditation are needed to determine whether a message should be classified as spam before it reaches the user. Independent authorities would manage the certification process and set the criteria. An oversight board, with cross-sector representation, would oversee the certification authorities.

Toward this end, the trusted email open standard (TEOS) has been created by the ePrivacy Group. TEOS grew out of ePrivacy's industry self-regulation programme that aims to separate legitimate e-mail from spam. TEOS goes beyond authentication and creates a trusted identity for e-mail senders based on signatures in e-mail headers. Unlike the authentication signatures of DKIM, the TEOS signatures are visible seals in messages, certifying that the sender meets specified criteria.

In order to reduce the problem of bulk e-mails erroneously filtered as spam, industry continues to discuss the efficacy of a bulk mail certification mechanism. For example, legitimate bulk mails could be identified at the ISP level with a label that is recognized by the server, thus enabling more confident use of e-mail filters. Several criteria could be used as input to the certification process, such as a commitment to strong privacy practices. For instance, France is working with its data protection agency (CNIL) towards a certification for senders who notify the use of client records.

Each ISP would maintain a whitelist of the certified clients. The proposal requires an agreement among ISPs on the certification process and involves no external intervention. However, the method would require a critical mass of ISP participation to be effective and would be based on trust among ISPs since there is no external oversight of the certification process. In addition, assigning a fixed number to the definition of bulk mail may be problematic. Crafty spammers could use multiple free e-mail accounts to send large quantities of spam, with each account sending a number just under the pre-defined bulk mail threshold.

7.13.3 Validation sender's server?

FFS.

7.13.4 PGP signatures

FFS.

7.13.5 System configuration

Industrial and individual-level security best practices for ports, firewalls, networks, routers, proxies, access, passwords, permissions key protection and software installation are examples of use of system configuration as anti-spam technology. By configuring one's system to block unwanted mail, one only captures a percentage of spam. However, as more and more systems install these mechanisms, spammers will certainly become more ingenious but it will also become less and less desirable to spam as there will be more obstacles to overcome. People spam now because it is simple, quick and cheap. As that changes – and hundreds of thousands of system administrators are working to change that situation – it will be harder to spam successfully.

7.13.6 Anti-virus tools

Anti-virus tools are important technologies that reduce the risk of spam e-mails infecting computer systems. Generally, harmful spam e-mails have potentially virus-initiating files attached. Anti-virus software can scan mailboxes and prevent virus infections.

Some ISPs are working to constantly monitor and update anti-virus application programming interface (API), VSAPI, with Exchange Server. This technology provides anti-virus scanning on user mailboxes to put scanning out to the network edge, reducing the impact of viruses and virus-tainted e-mail on network infrastructures. It is also possible to prevent infected e-mail from leaving an organization by scanning outgoing mail, in addition to incoming mail.

7.14 How to use this review of technologies and factors to consider

The utility of any tool(s) will be dependent on the needs, technical ability and the infrastructure of the user of the same tool. Tools are meant to be deployed at different parts across the system and for differing purposes. Users will have to consider their needs and strategies of defence in depth as they choose and deploy anti-spam tools. Tools themselves vary in maturity, efficacy, reliability and deployment. Some tools are more prone to false positives, some are more effective in certain areas, and some have greater overhead in terms of cost, infrastructure, bandwidth/capacity and needed technical expertise. A number of these factors have been listed for consideration, but users will have to gauge tools in the specific context of their contemplated application.

Some of the above tests are designed to fight spam, while others aim to prevent certain types of behaviour which pose a threat to security and fail to respect the resources of the platform to which mail is sent or simply do not comply with the accepted rules for sending electronic messages. When a rule is implemented after the receipt of the data constituting the message to be delivered, it remains to be decided how the message should be dealt with. This will obviously depend upon the results of the tests carried out. Some tests are more reliable than others and can therefore justify recourse to more drastic measures. Furthermore, it may be decided to carry out other and more expensive tests on certain messages.

The various options for dealing with a message depending on the location of the rule implemented are presented below.

7.15 Rejection in the SMTP session

The interest in such rejection lies in not taking charge of the electronic message, whose distribution remains the responsibility of the remote server, which has been advised of the situation. In addition, it saves bandwidth capacity, firstly because the message is not received and secondly because the remote server will not have to send a delivery status notification (DSN), the message generated in response to a rejection, see [b-IETF RFC 3461]) that the message might generate. The task of issuing such a non-delivery message is transferred to the sender.

However, this type of rejection means that it is not possible to keep a copy of the message (and therefore to retrieve a legitimate message that might not have been accepted, or simply to investigate a rejection).

Moreover, not all SMTP servers are currently able to run certain tests during the SMTP session. This is changing, however, with the increasingly common use of new products and in particular interfaces such as sendmail's "milter", the Postfix "policy server" or the future OPES which will be able to connect any program to the SMTP session.

7.16 Silent rejection

This method often confounds regular users who expect their e-mail to be delivered or at least to be told that it has been rejected. The "deliver or advise" alternative is a cardinal principle of e-mailing, but one which will probably have to be abandoned due to the large number of e-mails that purport to be sent by a user was not involved.

Ideally, a record should be kept of e-mails destroyed in this way so that techniques such as message tracking can be used, for example by deploying [b-IETF RFC 3885] describing the message tracking protocol, which allows users to learn what happened to their messages (like the parcel tracking systems of typical parcel delivery companies).

7.17 Rejection by sending a DSN (delivery status notification or "bouncing")

This is the method traditionally used in electronic mailing. However, due to the presence of joejobs, there is a risk of penalizing innocent senders, as may be seen with the anti-virus programs which mistakenly send DSNs.

7.18 Delivery to a spam box

When few messages are blocked on entry to the platform, the spam box can contain very large volumes of messages, which can discourage users from reading it. The message is not destroyed, but the user is given an opportunity to remedy false positives.

7.19 Marking

The server takes no decision but simply places a note on the e-mail. This technique gives the user full control, but will also force the user to download spam mail.

Note that an e-mail service provider could offer the user the choice of simply marking the e-mail or delivering it to the spam box. It is relatively simple to manage.

Appendix I

Activities on countering e-mail spam

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

I.1 Introduction

This appendix describes recent activities in the various organizations, including ITU-T, technical specifications, industry alliances and initiatives on countering e-mail spam. The organizations listed here are identified to show active relevant work on countering e-mail spam during the period of the Recommendation development. Therefore, the range and validity of technical specifications and the status of listed organizations may change in the future.

I.2 International activities on countering spam

I.2.1 ITU

In the Declaration of Principles adopted during the first phase of the World Summit on the Information Society (WSIS), held in Geneva in December 2003 [b-WSIS-2003], spam was identified as a potential threat to the full utilization of the Internet and e-mail services. Accordingly, WSIS participants recognized that spam is a "significant and growing problem for users, networks and the Internet as a whole" and that to build confidence and security in the use of ICTs, there is a need to "take appropriate action at national and international levels".

The interest of ITU Member States in issues relating to spam was highlighted during the ITU World Telecommunication Standardization Assembly (WTSA), held in Florianópolis, Brazil in October 2004. During the Assembly, ITU Members approved two resolutions relating to future ITU activities in the field of spam.

The first one, Resolution 51 on Combating Spam, instructs the Directors of ITU's three Sectors and the Secretary-General urgently to prepare a report to the 2005 Council on relevant ITU and other international initiatives for countering spam, and to propose – with the contribution of Member States and Sector Members – possible follow-up actions for consideration by the Council. The Resolution further invites Member States to take the appropriate steps within their national legal frameworks to ensure that appropriate and effective measures are taken to combat spam.

The second Resolution, Resolution 52 on Countering spam by technical means, affirms that "spam creates telecommunication network security problems, including being a vehicle for spreading viruses, worms, etc." The Resolution also recognized the availability of relevant ITU-T Recommendations, which could provide guidance for future development in this area, and therefore instructs the relevant ITU-T study groups – in cooperation with the Internet Engineering Task Force (IETF) and other relevant groups – to develop, as a matter of urgency, technical Recommendations on countering spam, as appropriate, and to report regularly to the Telecommunication Standardization Advisory Group on their progress. This effort should be supported by all necessary assistance from the Director of the Telecommunication Standardization Bureau, which will report to the ITU Council regarding the subject.

I.2.2 OECD

Spam is having a negative impact on the digital economy, and results in important economic and social costs for OECD and non-OECD countries. Given the potential for further problems as a result of the convergence of communication technologies and the emergence of ubiquitous communication and mobile Internet, OECD member countries are faced with the necessity of finding effective ways to combat spam. In order to meet this challenge, the OECD's Committee for Information, Computer and Communications Policy (ICCP) supported work on this important topic during the meeting on 3-4 March 2003, requesting that it be placed on a fast track, and noting that this was a global issue. The Committee on Consumer Policy (CCP) also expressed interest in pursuing OECD work on this topic. An initial exploration of issues linked with spam was undertaken in a background document and in a Workshop on Spam in February 2004, hosted by the European Commission in Brussels.

Spam is a cross-cutting issue impacting on network utilization, congestion issues and IP-based network issues; privacy and network security issues; and consumer protection issues. In order to better coordinate work on spam and assist in obtaining a more rapid consensus on a policy framework to tackle spam issues, the OECD Council agreed in July 2004 to set up a horizontal "Task Force on Spam". The Task Force was requested to report to the CCP and ICCP by July 2006.

The primary objective of the Task Force was to bring together designated anti-spam policy coordinators and allow for the most effective preparation of urgently needed policy tools to combat spam, approaching the problem in a broader way and benefiting from the multi-disciplinary expertise of OECD.

The Task Force was asked to study, document and promote the range of existing and emerging anti-spam strategies across all sectors. Recognizing that there is no "silver bullet" to tackle spam, the Task Force developed an Anti-Spam Toolkit ("the Toolkit") in April 2006. The Toolkit is based on the premise that a number of different coordinated elements need to be brought to bear on the problem of spam to help the development and growth of anti-spam strategies and solutions in the technical, regulatory and enforcement fields and to facilitate international cooperation. The OECD Toolkit is aimed at bringing together a set of consistent and complementary policy and other (e.g., enforcement) initiatives. The elaboration and implementation of the Toolkit relied substantively on the input of stakeholders in the various areas covered. The Toolkit is composed of eight interrelated elements:

– Anti-spam regulation.

– International enforcement cooperation.

– Industry-driven solutions against spam.

– Existing and emerging anti-spam technologies.

– Education and awareness.

– Cooperative partnerships against spam.

– Spam metrics.

– Global cooperation (outreach)

Background reports were prepared for the Task Force for several of the elements of the Toolkit. This appendix synthesises the work which has been undertaken by the Task Force and its conclusions. This appendix is complemented by the OECD Council Recommendation on Spam Cross-Border Enforcement Cooperation, and the OECD Anti-Spam website www.oecd-antispam.org.

I.2.3 APEC

In Asia-Pacific Economic Cooperation (APEC), spam-related issues are discussed in the Telecommunications and Information Working Group (TEL WG). The TEL WG is committed to improve the telecommunications and information infrastructure in the region and to facilitate effective cooperation, free trade and investment, and sustainable development.

In the area of the security of networks and infrastructure, TEL pursues cooperative work with other organizations on security issues, and strengthens work on creating a safe on-line environment in the information society, dealing with such issues as spam, to counter threats to the networks, including follow up actions on APEC Principles for Action Against Spam and the APEC Implementation Guidelines for Action Against Spam and cooperation with international and regional organizations such as ITU, OECD and the Association of South East Asian Nations (ASEAN). Related information is provided at the APEC TEL WG website (http://www.apectelwg.org/).

I.3 Development of technical specifications for countering spam

I.3.1 ITU-T

The World Telecommunication Standardization Assembly (Florianópolis, 2004), in Resolution 52, instructed the relevant study groups, in cooperation with IETF and other relevant groups, to develop technical Recommendations, including required definitions on countering spam, as appropriate, and to report regularly to the Telecommunication Standardization Advisory Group on their progress.

Study Group 17, as the lead study group on telecommunication security and in supporting the activities of WTSA Resolutions 50, 51 and 52, is well-positioned to study the range of potential technical measures to counter spam as it relates to the stability and robustness of telecommunication networks. ITU-T SG 17 established a dedicated rapporteur group, Q.17/17, for providing technical solutions on countering spam. The initial work is focused on developing technical specifications on countering e-mail spam. Later, the works are extended to develop technical solutions on countering spam for IP multimedia applications such as IP telephony, instant messaging, etc. Technical specifications cover or plan to cover guidelines, requirements, technical frameworks and technical means for countering various types of spam.

I.3.2 IETF

IETF has developed several RFCs on countering e-mail spam ranging from guidelines to technical specifications as follows:

– [b-IETF RFC 2505] "Anti-Spam Recommendations for SMTP MTAs":

  This RFC gives a number of implementation recommendations for SMTP MTAs (Mail Transfer Agents) to make them more capable of reducing the impact of spam. The intent is that these recommendations will help clean up the spam situation if applied on enough SMTP MTAs on the Internet, and that they should be used as guidelines for the various MTA vendors. This is not the final solution, but if these recommendations were included, and used, on all Internet SMTP MTAs, things would improve considerably and give time to design a more long-term solution. The future work section suggests some ideas that may be part of such a long-term solution. It might, though, very well be the case that the ultimate solution is social, political or legal, rather than technical in nature. The implementer should be aware of the increased risk of denial of service attacks that several of the proposed methods might lead to. For example, increased number of queries to DNS servers and increased size of logfiles might both lead to overloaded systems and system crashes during an attack.

– [b-IETF RFC 2635] "DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)":

  This RFC explains why mass unsolicited electronic mail messages are harmful in the networking community. It gives a set of guidelines for dealing with unsolicited mail for users, for system administrators, news administrators and mailing list managers. It also makes suggestions that internet service providers might follow.

– [b-IETF RFC 3685] "SIEVE Email Filtering: Spamtest and VirusTest Extensions":

  The SIEVE 'spamtest' and 'virustest' extensions permit users to use simple, portable commands for spam and virus tests on e-mail messages. Each extension provides a new test using matches against numeric 'scores'. It is the responsibility of the underlying SIEVE implementation to do the actual checks that result in values returned by the tests.

– [b-IETF RFC 4686] "Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)":

  This RFC provides an analysis of some threats against Internet e-mail that are intended to be addressed by signature-based mail authentication, in particular DomainKeys identified mail. It discusses the nature and location of the bad actors, what their capabilities are, and what they intend to accomplish via their attacks.

In addition to those, several drafts are in development describing domain-level authentication which are applicable to countering e-mail spam.

I.4 List of industry alliances and initiatives for countering spam

Below is a list of industry initiatives from around the world. It is non-exhaustive and should be interpreted as an attempt to illustrate the rich variety of projects being undertaken by various organizations in order to fight spam in a more coordinated and effective manner.

I.4.1 Anti-Phishing Working Group

The Anti-Phishing Working Group (APWG) [b-APWG] is the global pan-industrial and law enforcement association focused on eliminating fraud and identity theft that result from the growing problem of phishing, pharming and e-mail spoofing. The organization provides a forum to discuss phishing issues, defines the scope of the phishing problem in terms of hard and soft costs, and shares information and best practices for eliminating the problem. Where appropriate, the APWG will also look to share this information with law enforcement.

I.4.2 Authentication and Online Trust Alliance

Founded in October 2004, E-mail Authentication.org has evolved into the Authentication and Online Trust Alliance (AOTA Inc.). The mission of AOTA is to enhance online trust and confidence in all forms of electronic messaging, e-commerce, e-banking and the internet, helping to improve safety and online protection of businesses and consumers alike. The goals include facilitating best practices, data sharing and deployment and implementation of e-mail and Internet authentication, identity and reputation standards and solutions and domain defence strategies, providing the ecosystem prescriptive and actionable advice in a vendor-neutral environment. AOTA is comprised of leading business, industry and non-profit organizations who are working to improve trust and confidence in electronic messaging, the Internet and e-commerce. With the onslaught of phishing and forged e-mail, this collaboration is critical to help ensure the reliability and deliverability of e-mail, reinforce online trust and confidence, and protect the brands and domains of businesses worldwide.

In early 2004, a group of business, industry and marketing leaders led by Bigfoot Interactive, Email Sender and Provider Coalition (ESPC), Microsoft and Sendmail began meeting to pursue solutions to authenticate e-mail and improve user confidence. Following the U.S. Federal Trade Commission's Authentication Summit in November 2004, which was co-sponsored with the Department of Commerce's National Institute of Standards and Technology, a decision was made to take decisive action to advance authenticated email, forming emailauthentication.org. With the continued onslaught of phishing and deceptive email undermining user and business confidence, in September of 2006, emailauthentication.org was incorporated as the AOTA.

While maintaining its focus and technical leadership in e-mail authentication, AOTA's mission was expanded to help address boarder issues and threats impacting online trust and confidence.

I.4.3 Contact Network of Spam Authorities (CNSA)

On the initiative of the European Commission, an informal group was created consisting of National Authorities involved with the enforcement of Article 13 of the Privacy and Electronic Communication Directive 2002/58/EC called "the Contact Network of Spam Authorities (CNSA)".

In the CNSA, information on current practices to fight spam is exchanged between National Authorities, including best practices for receiving and handling complaint information and intelligence and investigating and countering spam. The Commission is responsible for the CNSA secretariat. The CNSA is further assisted by a coordinator. The coordinator facilitates information exchange between CNSA members and supports the Commission's secretariat. The current coordinator is France's Prime Minister's Office. The CNSA meets on a regular basis (3-4 times per year) in Brussels. The CNSA also holds joint meetings with the London Action Plan annually.

The CNSA has set up a cooperation procedure that aims to facilitate the transmission of complaint information or other relevant intelligence between National Authorities.

I.4.4 Digital PhishNet

Digital PhishNet (DPN) was established on December 8, 2004, as a collaborative enforcement operation to unite industry leaders in technology, banking, financial services and online auctioneering with law enforcement to combat "phishing", a destructive and growing form of online identity theft.

Phishing is a particularly harmful and deceptive emerging online threat that involves directing consumers to phony websites, usually through forged or "spoofed" spam e-mails, to input personal financial information such as credit card numbers and passcodes. While other industry groups have focused on identifying phishing websites and sharing best practices and case information, DPN is the first group of its kind to focus on aiding criminal law enforcement and assisting in apprehending and prosecuting those responsible for committing crimes against consumers through phishing. DPN establishes a single, unified line of communication between industry and law enforcement, so critical data to fight phishing can be compiled and provided to law enforcement in real time.

I.4.5 Email Sender and Provider Coalition

The Email Sender and Provider Coalition (ESPC) is a cooperative group of industry leaders working to create solutions to the continued proliferation of spam and the emerging problem of deliverability. The ESPC members have recognized the need for strong spam solutions that ensure the delivery of legitimate e-mail and have been very active in the war against spam. The ESPC works on solutions to spam and deliverability concerns through a combination of legislative advocacy, technological development and industry standards.

The ESPC is comprised of four sub-committees:

– Legislative – Guides ESPC's lobbying efforts on federal and state spam legislation.

– Receiver relations – Formed to help facilitate better understanding and ongoing dialogue between the sender community and the established receiver community.

– Technology – Evaluates and develops technological solutions that would allow more accurate responses to spam (and fewer false positives). A technical working group has been formed within this group to explore and propose such solutions. This group meets as needed, with in-person meetings scheduled occasionally.

– Communications – Provides broad public affairs strategy for the coalition.

I.4.6 Institute for Spam and Internet Public Policy (ISIPP)

The Institute for Spam and Internet Public Policy (ISIPP) is dedicated to providing analysis, information and consulting on industry issues relating to public policies and processes regarding spam, e-mail, e-mail deliverability and the Internet. ISIPP also provides a widely-used e-mail sender accreditation service, SuretyMail, and organizes and sponsors industry forums such as e-mail management roundtables, e-mail deliverability summits and the "Spam and the Law" conferences.

I.4.7 London Action Plan

The London Action Plan is a global network of law enforcement agencies and industry representatives involved in the fight against spam, phishing and related online threats. The U.S. Federal Trade Commission and the UK's Office of Fair Trading spearheaded the creation of the London Action Plan in 2004. The London Action Plan now has members from over 20 countries. Since its inception, the London Action Plan has fostered both bilateral and multilateral relationships among law enforcement agencies, thereby facilitating international cooperation in several spam investigations. In 2005, the London Action Plan collaborated with several other government partners in "Operation Spam Zombie", an initiative in which agencies all over the globe sent letters to Internet service providers urging them to employ protective measures to prevent consumers' computers from being hijacked to send spam.

As mentioned above, the London Action Plan holds joint meetings annually with the CNSA. Most recently, the London Action Plan held its third joint workshop with the CNSA on October 9-11, 2007, in Washington, D.C. The LAP-CNSA workshop was held in conjunction with the 11th General MAAWG meeting. The LAP and CNSA held several joint sessions with MAAWG that focused on many relevant topics.

During the 2007 workshop, the London Action Plan also held training sessions for law enforcement agencies, explored the benefits of public-private cooperative initiatives, and addressed ways to enhance cross-border enforcement cooperation. Law enforcement and private sector representatives from over 20 countries attended the joint workshop.

I.4.8 Messaging Anti-Abuse Working Group (MAAWG)

The Messaging Anti-Abuse Working Group (MAAWG) is a global organization focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages. With a broad base of Internet service providers (ISPs) and network operators representing over 600 million mailboxes, key technology providers and senders, MAAWG works to address messaging abuse by focusing on technology, industry collaboration and public policy initiatives.

The purpose of MAAWG is to bring the messaging industry together to work collaboratively and successfully address forms of messaging abuse such as messaging spam, virus attacks, denial-of-service attacks, and other forms of abuse. To accomplish this, MAAWG is developing initiatives in the three areas needed to resolve the messaging abuse problem: collaboration, technology and public policy.

I.4.9 Spamhaus

The Spamhaus Project is an international non-profit organization whose mission is to track the spammers, spam gangs and spam services to provide dependable real-time anti-spam protection for IP-based networks, to work with law enforcement agencies to identify and pursue spammers worldwide, and to lobby governments for effective anti-spam legislation. Founded in 1998, Spamhaus is based in Geneva, Switzerland and London, UK and is run by a dedicated team of 25 investigators located in nine countries.

Spamhaus publishes the Register Of Known Spam Operations (ROKSO) – a database collating information and evidence on the '200' known worst spam gangs worldwide, used by ISPs to avoid signing up known spammers who would abuse their networks and by law enforcement agencies to help target and mount prosecutions against professional spammers.

Spamhaus publishes a number of real-time spam-blocking databases, including the Spamhaus Block List (SBL), the Exploits Block List (XBL) and the Policy Block List (PBL). Broadcast from a network of 40 DNS servers in 17 countries, the Spamhaus blocklists are used by many of the Internet's major Internet service providers, corporations, universities, governments and military networks.

Funding for operations is through sponsors and donations. Funding of international infrastructure is raised from the provision of a spam blocklist synchronization service ('Spamhaus Data Feed') supplied by a separate logistics organization to large IP-based networks and commercial spam filter companies.

I.4.10 Stop Spam Alliance

The Stop Spam Alliance is a joint initiative to gather information and resources on combating spam. This initiative was undertaken by APEC, the EU's CNSA, ITU, the London Action Plan, OECD and the Seoul-Melbourne Anti-Spam group.

In line with the WSIS Tunis Agenda [b-WSIS-2005] – asking members to "deal effectively with the significant and growing problem posed by spam" and calling upon all stakeholders to adopt a multi-pronged approach to counter spam – the Stop Spam Alliance pages link to initiatives in the field of anti-spam legislation and enforcement activities, consumer and business education, best practices and international cooperation.

A "common agenda of events", featuring the international events on spam and relating threats organized by the involved organizations is also available. The available website is http://stopspamalliance.org/.

I.4.11 Trusted Electronic Communications Forum (TECF)

The Trusted Electronic Communications Forum (TECF) is a cross-industry, cross-geographic consortium dedicated to the standardization of technologies, techniques and best practices in the fight against phishing, spoofing and identity theft. The focus of the TECF is to efficiently and effectively create, deploy and endorse solutions to problems presented by research studies, analysts and by its members. Working groups and committees are sponsored to formulate and/or validate techniques and tools that specifically address high-risk threats outlined by the TECF.

Bibliography

[b-WSIS-2003] WSIS First Phase (2003), *Declaration of Principles*.
<http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160>

[b-WSIS-2005] WSIS Second Phase (2005), *Tunis Agenda for the Information Society*.
<http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|2267>

[b-APWG] Anti-Phishing Working Group, <http://www.antiphishing.org/>.

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*.
<http://www.ietf.org/rfc/rfc2505.txt>

[b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)*.
<http://www.ietf.org/rfc/rfc2635.txt>

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*.
<http://www.ietf.org/rfc/rfc2821.txt>

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format*.
<http://www.ietf.org/rfc/rfc2822.txt>

[b-IETF RFC 3461] IETF RFC 3461 (2003), *Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)*.
<http://www.ietf.org/rfc/rfc3461.txt>

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions*.
<http://www.ietf.org/rfc/rfc3685.txt>

[b-IETF RFC 3885] IETF RFC 3885 (2004), *SMTP Service Extension for Message Tracking*.
<http://www.ietf.org/rfc/rfc3885.txt>

[b-IETF RFC 4686] IETF RFC 4686 (2006), Analysis of Threats Motivating DomainKeys Identified Mail (DKIM).
<http://www.ietf.org/rfc/rfc4686.txt>

[b-FTC] United States Federal Trade Commission, *Email Address Harvesting and the Effectiveness of Anti-Spam Filters*, November, 2005.
<http://www.ftc.gov/opa/2005/11/spamharvest.pdf>

[b-Lyris] Lyris Technologies, Inc., *Email Advisor: ISP Email Deliverability Report Card*, 2nd quarter, 2007.
<http://www.lyris.com/resources/reports/deliverability_report_Q22007.pdf>

[b-OECD TF] OECD Task Force on Spam (2006), *Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures*.
<http://www.oecd.org/dataoecd/63/28/36494147.pdf>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009