Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2013) 21: 2259 – 2268

doi:10.3906/elk-1112-55

Stopping spam with sending session verification

Ahmet BARAN*
Department of Computer Technologies, Erzincan University, Vocational High School, Erzincan, Turkey

Received: 14.12.2011 • **Accepted:** 23.07.2012 • **Published Online:** 30.10.2013 • **Printed:** 25.11.2013

Abstract: Spam has become one of the most significant problems for Internet communication and users today. The traditional filtering methods and signature-based spam blocking systems that have come into prominence recently fall short, as statistics demonstrate that spam further mounts up day after day. In this study, a new method is recommended to block spam mails. In this recommended method, a mail sending session is verified during mail envelope communication by adding small attachments to the simple mail transfer protocol, so spam mails can be blocked before leaving the sender domain or relay machine. Additionally, hijacked user accounts are able to be detected by statistical filtering software support, and spam mails coming from these users can be blocked and the account owners can be informed. According to the test results, 99.4% of the spam mails were able to be stopped by the proposed method, and the false positive problem was able to be solved and a significant decrease in the false negative percentages was ensured.

Key words: Electronic mail, SMTP improvements, antispam, session verification

1. Introduction

Today, e-mail communication occupies quite an important space in our daily lives. Additionally, e-mails called spam have turned into an important problem for Internet users and they even threaten the future of the Internet system. Spam mails cause considerable damage to companies and their employees, e-trade environment, customers, Internet services providers (ISPs), email service providers (ESPs), and public institutions.

States attempt to take legal precautions enacting various regulations to block spam that leads to massive financial losses and the violation of laws [1,2]. On the other hand, a great many methods were proposed to block spams in academic and commercial circles and are being used [3–6]. However, these methods fall short, as statistics report that spam amounts have been increasing each day. According to the statistics of the Symantec Intelligence Report, while spam mails constituted 8% of the total e-mail traffic in 2001, they constituted 70% in 2005 and 77.8% as of July 2011 [7].

Considering the recipients, a recipient receives a lot of e-mails that he/she does not want each day. Mail recipients are spammed by spammers exploiting the shortcomings of the still used simple mail transfer protocol (SMTP) system using the following 5 methods:

They receive a great deal of e-mails:

- From an inexistent domain,
- A spam distributing domain,
- An existent domain but an inexistent e-mail address,

*Correspondence: baran@erzincan.edu.tr

- An existent domain and e-mail address, but not sent from that particular e-mail address,
- An existent domain and e-mail address, sent from that particular e-mail address, but the e-mail owner is not aware of that mail

The objective of antispam techniques is to block these unwanted mails and their approach styles vary. There is still no technique that can block all of these mentioned methods of spammers in the literature; many of the used blocking methods cannot prevent the most important damage of spam (such as bandwidth use, storage cost).

In this study, a spam blocking system is proposed that is based on reciprocal controls and informing in order to block all of these methods of spammers. The suggested method is a developed version of a combination of the sender policy framework (SPF) [8], bounce address tag validation (BATV) [9], and domain key identified mail (DKIM) [10] signature-based methods and statistical filtering. In this method, domains broadcast an address record in their domain name system (DNS) servers as in the SPF method. Unlike the SPF method, this record does not include the Internet protocol (IP) of the server having authority to the send mail; it includes the IP of a verification server (VS) with which the receivers can make an inquiry of the mail sending session. In the suggested method, by making the mail sending session verification during the envelope communication by means of the VS, it is decided whether the mail is legitimate or spam. In the suggested method, in order to make session control, which is different from the BATV method where the local parts of the mails are modified, small changes are suggested in the SMTP communication. The method works on the basis of the verification of the unique session ID and the receiver and sender mail addresses, and the authenticity of the message is ensured with the usage of the DKIM method. At the same time, the method is operated in combination with a statistical filtering method in the receiver mail server in order to distinguish the mails being sent from hijacked accounts and to provide a notification to the sender mail server.

This method is a way that merges the mentioned methods and it differentiates from studies in the literature in 2 ways. In the first one, a vast majority of spam mails can be blocked before leaving the sender domain or relay by making a sending session verification in the course of the mail communication, which is different from techniques available during envelope communication in the literature. The second feature of the system, which we know is not in the literature, is to be able to inform the sender domain and user by providing feedback to the sender domain as a result of the e-mail communication for the purpose of blocking e-mails spreading from the hijacked user accounts.

The remainder of this paper is structured as follows. Section 2 gives some information about the behavior of spammers and antispam techniques. In Section 3, we describe our approach, and Section 4 gives the results and details of our system's experimental test bed implementation. We provide our conclusions in Section 5.

2. Spammers and antispammers

2.1. Behavior of spammers

The most critical element for spam mail senders is that they cover their tracks. Therefore, spammers do not directly send spam mails. Instead, they send either by hijacking others' computers or accounts and using these computers or computers that were inaccurately configured on the Internet, or using Internet connections that cannot be followed.

A vast majority of spams today spread out from networks comprised of hijacked computers that are called bots or zombies and are controlled by spam operators [11,12]. Another widespread method that spammers use to hide their identities is to use open proxies [13]. Having said that, spammers usually use servers called mail relays

to profit from their time and effort [14,15]. On the other hand, there are plenty of methods for accessing the Internet without using an individual or fixed physical connection and they cannot be followed. Internet cafes; illegal wireless connections; campus networks, in which the control and log mechanisms of many universities are not operated; and Internet access from ISPs by aliases and untraced payment methods can be given as examples for these methods. In such situations, spammers can spread spam without hiding their identities or using the aforementioned methods [16].

2.2. Operations of antispammers

There are a variety of antispam techniques. We classify them into 3 groups: filter-based approaches, signature-based approaches, and other approaches. Each class of approaches has its own advantages and disadvantages. Under specific circumstances, 2 or more approaches may work more effectively when they work together.

In nonstatistical filtering methods, the classic blacklist, whitelist, and graylist approaches are employed [17]. A great deal of content analysis-based statistical filter methods have been recommended for fighting spam. The main content analysis studies are naïve Bayes, support vector machines, artificial neural networks, logistic regression, lazy learning, artificial immune systems, boosting, ensembles, image analysis, and hybrid methods. The authors in [3–5] classified and evaluated these methods in their studies.

Spam mails are attempted to be blocked by trying to determine the sender's identity in signature-based methods. Secure/multipurpose Internet mail extensions (S/MIME) [18], OpenPGP [19], BATV [9], DKIM [10], certified server validation (CSV) [20] and sender policy framework [8] + sender ID framework (SPF + SIDF) [21] methods are principal signature-based methods. The authors in [6] and [22] examined these methods and assessed their shortcomings.

On the other hand, transmission control protocol blocking, verification, payment-based, limitation of outgoing mails, address obscuring techniques, and reputation-based methods are some of the other methods recommended for blocking spams [4].

3. Recommended system

Considering the mail sender, a sender writes his/her e-mail using a mail transfer agent (MTA) or mail user agent (MUA) in a formal SMTP communication. The prepared e-mail is sent to the organization's MTA, either directly by intraorganization SMTP communication or over the Webmail server via the hypertext transfer protocol secure HTTP(S) protocol. The last MTA in the sender's organization (SO) can either connect to the MTA of the receiver's organization (RO) via the SMTP or make a SMTP connection to another server on the Internet. This server can be a mail relay or a gateway. After using a mail relay or gateway one time, mail can pass through many relay or gateway machines until it reaches the MTA of the RO. The RO can use more than one MTA as the SO and the last MTA sends e-mail to a mail delivery agent (MDA) for it to be stored. The receiver accesses the message using post office protocol or Internet message access protocol, in general, by a MUA [23].

That being said, e-mail communications following quite distinct ways other than the one explained above are also possible [4] and spammers usually employ these methods. Spammers, who connect to the Internet by bots and untraceable connections, send spam mails with a MTA or MUA via either connecting to the MTA of a RO or over a SMTP relay. Spammers possessing traceable connections send spams to receivers by necessarily passing over a gateway. The common point of sending such e-mails is that these e-mails are sent without passing over the MTA of the sender's domain. Port blocking (e.g., Port 25) is a quite frequently used method for the

purpose of canceling mail sending without passing over the domain MTA by computers on a domain and it is used in this study as well [24]. Considering the sender's domain, this method cuts most of the spam sent from the domain, except for that bot software, which accesses the ESP user information, using the way that direct legal e-mails use. As for the receiver's domain, it has no use in the name of the sender's domain due to the fact that they make domain spoofing by computers on other domains.

In a nutshell, considering the receiver, an incoming e-mail can be sorted into 2 categories: mails that pass over the sender's MTA and ones that do not. The first point recommended in the method proposed in this article is to discard e-mails that do not pass over the sender's MTA and only take into account the ones that do pass over the sender's MTA. To understand which e-mails pass over the sender's MTA, a VS is recommended in which the logs in the sender's domain are kept in a special format. The second suggested point is to rate the domain e-mail users in the sender's domain through feedback coming from other domains with respect to e-mails that they sent.

The system recommended in this method has the structure in Figure 1. The address verification system, which is not available in the standard e-mail communication system currently used hardware-wise, is recommended in the schema. The function of this server for small- and medium-range ESPs can be fulfilled in the domain MTA server as well. Nevertheless, a number of small additions are made to the existent SMTP for goals to be realized in terms of operation.

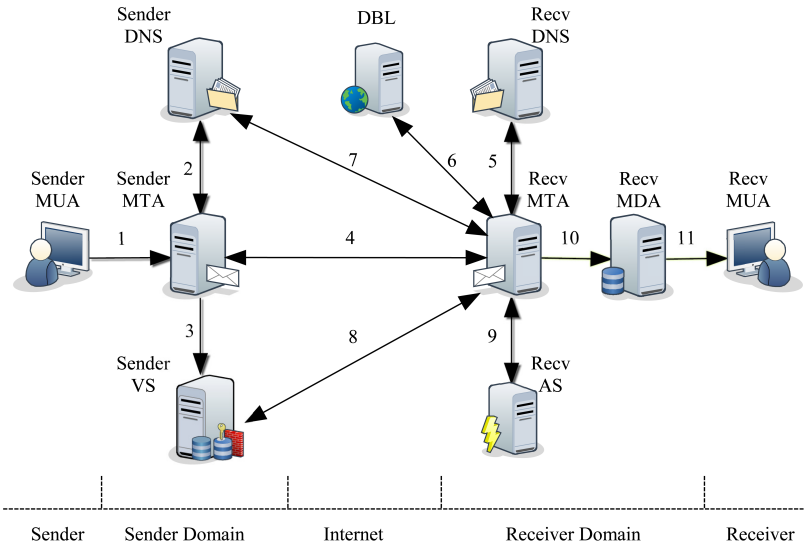

Figure 1. Recommended e-mail communication schema.

The sender in the recommended schema sends e-mail to the MTA of the sender's domain with an internal SMTP client after preparing e-mail (1). If there is more than one MTA in the sender's domain, the MTA here refers to the last MTA. The sender's MTA (SMTA) questions either the DNS server that the domain has or the previously configured DNS server to learn IP information of the target domain, by first determining the target domain from the incoming e-mail information (2). When the DNS server gets back to the SMTA as a result of the query, the SMTA responds in 2 ways with regard to the incoming response.

If the DNS query result is successful (if the receiver domain is available), the SMTA commands the VS to insert a record, whose structure is given in Table 1 (3). This record consists of a local timestamp, a unique ID value given to every e-mail, the sender's e-mail, receiver's e-mail, IP address of the authorized questioning,

sender rating, and result of the mail. However, the first 4 in the list are still kept as standard in many e-mail sending software, and the last 3 are key for the method recommended in this study. An authorized IP address is the IP address of the reliable relay machine or the receiver's MTA (RMTA) obtained as a result of the DNS query. The VS records a rating value on the space of the sender's rating of the record by calculating it with respect to previous e-mail sending statistics of the owner of the sender e-mail in the record's insert. The calculation and use of the rating value will be explained later. Moreover, the space of the result of the mail, on which the evaluation result of the e-mail sending operation in the receiver's domain is written, is kept in this record. Here, another critical point is that a separate record is added for each receiver when there is more than one mail receiver.

Table 1. Structure of the logging table in the VS.

Timestamp	Unique ID	Sender e-mail	Receiver e-mail	IP address of authorized questioning	Sender rating (%)	Result of mail

If the DNS query result is unsuccessful (if there is no receiver domain) or the communication is terminated due to queries made by the RMTA after this point, the SMTA commands the VS to update the rating value of the sender user with the thought that it sent spam.

Accompanying the formation of the record in Table 1, the VS either informs its internal or the institution's firewall that the IP in the record has the authorization of access. After this command, a record as in Table 2 is added to the firewall. This record holds the information of the *message ID*, *IP address of the authorized questioning*, and the *last validity time* of record. With the addition of the record, the firewall allows access of the respective IP to the VS and erases the record when its last validity time arrives. The objective of the firewall here is to create a tunnel that can block unnecessary and malicious queries of the VS database, in big ESPs in particular. The period of the last validity time info is 48 h, as a default, and it can be changed with respect to the institution policies.

Table 2. Rule record of the firewall of sender domain.

Message ID	IP address of authorized questioning	Last validity time

At this juncture, the SMTA communicates with the RMTA (4). The RMTA, when it receives the request, queries either its own domain server or other DNS servers on the Internet to first understand whether that domain exists and find out the domain's DNS server (5). If the sender domain cannot be found, then it terminates the connection. Afterwards, it queries the respective domain from reputation servers on the Internet (6). It continues or terminates the connection based on the result of the incoming information. The Spamhaus domain block list (DBL) database [25] is used in the recommended method in this study to detect spam-only servers.

For continued communication, the RMTA requests the *mail from*, *mail to*, and *unique ID* information from the SMTA. While the mail to and mail from information is used in the ongoing SMTP communication, the system makes an addition to the conversation part of the SMTP communication here. The recommended SMTA conversation should be step by step and in order, as in Figure 2. Accordingly, after checking the existence of the sender's domain and reputation, the RMTA first waits for the sender and receiver information from the SMTA. In the wake of receiving the sender and receiver information, whether the receiver is situated on the

domain is checked. If the receiver is not situated on the domain (possibility of directory attack), the connection is terminated. If the receiver presents on the domain, the RMTA sends 250 OK to the SMTA. Following this message, the RMTA awaits either the *unique ID* or *DATA* information from the SMTA. If the SMTA sends a *DATA* message, the RMTA sets the spam score of the e-mail to a predetermined K value, assuming that the sender's domain does not use this control scheme.

<table>
<tr><td>R.
S.

R.
S.
R.
S.
R.

</td><td colspan="2">220 receiverdom.com
HELO senderdom.com
if (senderdomain not exists) then reply with 554
else
if (senderdomain in DBL) then reply with 554
else
250 receiverdom.com
MAIL FROM: sender@senderdomain.com
250 Ok.
RCPT TO: receiver@receiverdom.com
if (receiver not exists) then reply with 554
else
250 Ok.</td><td>STAGE 1
STAGE 2
STAGE 3</td></tr>
<tr><td>S.

R.
S.

SpamScore = SenderRating</td><td>UNIQUEID: EH7YG9K12
if (uniqueid is not verified from VS) then reply with 554 else
250 Ok.
DATA</td><td>

DATA
SpamScore = K</td><td>STAGE 4
STAGE 5</td></tr>
<tr><td>R.
S.
S.
S.
R.

R.
S.
R.</td><td colspan="2">354 enter mail, end with line containing only "."
Subject : Hello
Hello, can you call me?
.
250 Ok. Queued as receivermsgid.
SpamScore + = CAS Result
if (SpamScore ≥ Threshold Value) then
mark as spam
else mark as legitimate
250 Ok. Mail is received with "marked" value
QUIT
221 Bye</td><td>STAGE 6</td></tr>
</table>

Figure 2. Stages of the recommended SMTP conversation.

If the SMTA sends a *unique ID* message and info to the RMTA, the RMTA queries the DNS server of the sender's domain that it obtained at the fifth step (7). In the recommended method, the sender's domain issues the IP address information of the VS in the DNS server. If the IP information record of the VS machine is not available in the sender's domain DNS server, the RMTA terminates the connection. After learning the VS's address, the RMTA sends the *Message ID* information to this server for query (8). If the RMTA cannot connect to the VS server, it terminates the SMTA connection (due to reasons such as firewall access). After the RMTA connects to the VS server, the VS queries the *unique ID* value that it acquired from the incoming query in the database. If any record cannot be found or there is an IP incompatibility, the VS responds negatively to the RMTA, and then the RMTA sends a no to the SMTA, assuming with this response that the e-mail is fake and terminates connection. If any record is found and the IP of an inquirer is compatible with the IP in the record, the *sender address*, *receiver address*, and *sender rating value* in the record are sent to the RMTA (8). At this stage, the RMTA compares the information arriving from the VS and the SMTA. If there is no compatibility, the connection is terminated and in the case of any compatibility, the spam score of the e-mail is

set to the *sender rating value*. In this article, the ethical convenience of sending an individual's rating value to the ones he/she communicates with e-mail is not of interest.

If there is compatibility or the SMTA directly sends the *DATA* message to the RMTA, the RMTA requests the mail data from the SMTA (354 messages). At this juncture, the SMTA adds a signature to the mail header by calculating one from the mail body and the selected header information using one of the RSA-SHA1 and RSA-SHA256 algorithms, as identified in [10], to guarantee the integrity and accuracy of the mail content. Afterwards, the SMTA sends the mail data to the RMTA (header and body). If the sender used the recommended method and an encrypted signature (DKIM signature) was used in the e-mail, the signature is decrypted by the public key attained as a result of the DNS query. Hence, the sender's DNS server should issue a public key as identified in [10]. The obtained value and hash value of the mail data are compared. If there is no compatibility, it sends an error message to the sender, assuming that there was a change in the mail data, and terminates communication.

Subsequently, mail data and information are sent to content analysis software (CAS) in the receiver's domain to conduct a content analysis (9). CAS (for instance, Spamassassin [26]) sends evaluation results regarding whether e-mail is spam to the RMTA by employing statistical methods. The RMTA obtains a final SpamScore by assembling the previous SpamScore and this info. If the SMTA sent a *unique ID* (if using the method), the RMTA sends an e-mail SpamScore to the VS. The VS updates the result of the mail information of the respective record, and transfers the record to the archive database and shuts down firewall access. On the other hand, the RMTA marks the e-mail as reliable or suspicious with regard to the SpamScore and sends it to the receiver MDA (10). Here, the *from* space in the body part and *sender email* information acquired during the envelope communication are compared to prevent phishing and if there is a difference, the *from* space is changed with the sender email and the *from* space information is given as information in the body data of the e-mail. Finally, the e-mail is delivered from the RMTA to the receiver MUA (11).

The objective of carrying out the statistical analysis of the e-mails in the system is to detect hijacked user accounts. It is used with the aim of informing the SO for the detection of computers that send e-mail from user accounts without the will of the users. Accordingly, the resulting value of the statistical analysis operation is sent to the VS by the RMTA in the sender's domain. In our study, an effective spam zombie detection system named SPOT [27] is employed for the user rating. The SO that rates the mail users with the returning feedback information may resort to informing these users by blocking the hijacked or maliciously used accounts. On the other hand, the system administrators, who do not want to trust the evaluation criteria and threshold of the receiver domains on the Internet, can calculate and get this operation per se by processing each outgoing e-mail in the domain in a CAS machine.

4. Experimental results

A structure as in Figure 3 was constituted to test the recommended system. A VS server was configured in domain A for the verification operation and the database, whose structure is presented in Table 1, was run on the MYSQL database server. Endian firewall software with an open source code [28] was configured in the VS entry and it is operated on the structure of the record, as in Table 2. The sender's domain (domain A) publishes the IP address of the VS and DKIM public key in the records of the domain name server. MTA-A and MTA-B were configured by the open source Postfix [29] software to ensure the SMTP communication stated in the previous section.

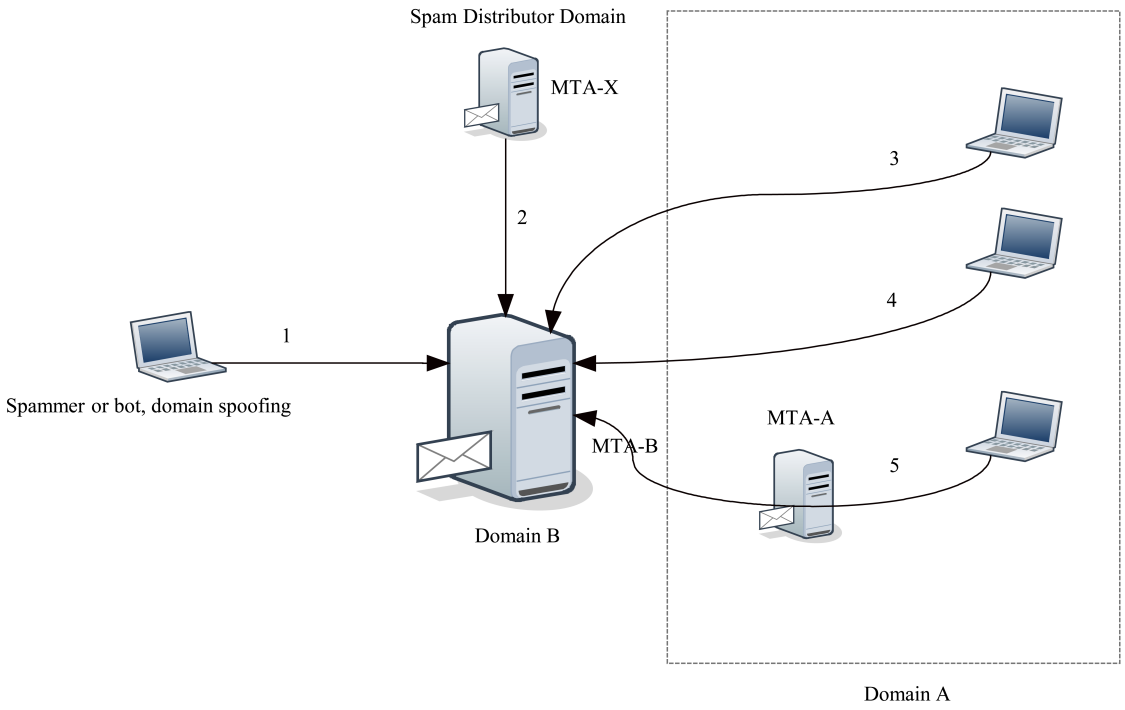

Figure 3. Structure of the testbed.

The 5 spamming methods explained in the first section were tested in the following configuration. No. 1 represents a mail sending request from an inexistent domain (or domain spoofing), no. 2 represents a mail sending request from a spam-only domain, no. 3 represents a mail sending request from a mixed domain but a fake (inexistent) e-mail account, no. 4 represents a mail sending request from a mixed domain with a real e-mail user name but one that in reality does not come from its user, and no. 5 represents a mail sending request from a mixed domain with a real e-mail user name and account but without its user's notice. The test results with regard to these possibilities are presented below.

As seen in Table 3, all of the spam mails coming from the first 4 ways were able to be blocked successfully. The first 3 mails coming from no. 5 could not be stopped (but were marked as spam) and the rest were able to be blocked. Hence, considering the spam mails coming from all of the ways, 99.4% of the spam mails were able to be blocked in the suggested method.

Table 3. Test results.

Way	Sent mails	Number of stopped mails in Suggested SMTP stages						False positive	False negative
		1	2	3	4	5	6		
1	100	100	-	-	-	-	-	0	0
2	100	-	100	-	-	-	-	0	0
3	100	-	-	-	100	-	-	0	0
4	100	-	-	-	100	-	-	0	0
5	100	-	-	-	-	-	97	0	3

Here, if the e-mails represented in no. 2 were considered to be sent from a spam-only domain that does not exist in the DBL list, and even though this domain does not use the recommended method, 97% of these

mails could still be blocked at the sixth stage. Having said that, in a case where that number of spams coming from a domain via both no. 5 and no. 2 increases, the receiver's domain resorts to include these domains in the blacklist by generating its own DBL.

5. Conclusions

Although various methods have been developed to block spam mails, the number of these mails soars day by day. This case stems from spammers changing their behaviors by figuring out the shortcomings of the protocols and antispam methods. Therefore, it is obvious that a secure end-to-end e-mail communication in a large network, such as the Internet, can only be ensured by mutual controls that will be conducted both for the sender and the receiver. The antispam method recommended in this study indicates that domains can safely communicate with each other with e-mail after carrying out mutual controls. For this purpose, the current SMTP protocol, which falls short now, needs to be updated. On the other hand, there is still no alternative to the reputation servers of today in the detection of spam spreaders and these servers carry a big responsibility on their shoulders. Additionally, sender domains should examine outgoing e-mails and receiver domains should examine incoming e-mails by performing content analysis to block spams spreading through hijacking user accounts.

References

[1] European Parliament and of the Council, Directive 2002/58/EC, 2002.

[2] United States Congress, Public Law 108187, 2003.

[3] J. Carpinter, R. Hunt, "Tightening the net: a review of current and next generation spam prevention tools", Computers and Security, Vol. 25, pp. 566–578, 2006.

[4] G. Schryen. Anti-Spam Measures, Analysis and Design, New York, Springer, 2007.

[5] T.S. Guzella, W.M. Caminhas, "A review of machine learning approaches to spam filtering", Expert Systems with Applications, Vol. 36, pp. 10206–10222, 2009.

[6] A. Herzberg, "DNS-based email sender authentication mechanisms: a critical review", Computers and Security, Vol. 28, pp. 731–742, 2009.

[7] Symantec Cloud (Message Labs), Research reports, available at http://www.symanteccloud.com, 2011.

[8] Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, IETF Documents, available at http://tools.ietf.org/html/rfc4408, 2006.

[9] Bounce Address Tag Validation (BATV), IETF Documents, available at http://tools.ietf.org/html/draft-levine-smtp-batv-01, 2008.

[10] DomainKeys Identified Mail (DKIM) Signatures, IETF Documents, available at http://tools.ietf.org/html/rfc4871, 2007.

[11] A.K. Seewald, W.N. Gansterer, "On the detection and identification of botnets", Computers and Security, Vol. 29, pp. 45–58, 2010.

[12] E.S. Mitchell, "Characterizing bots' remote control behavior", Proceedings of the 4th International Conference on Detection of Intrusions and Malware and Vulnerability Assessment, pp. 89–108, 2007.

[13] P.H.C. Guerra, D. Guedes, W. Meira, C. Hoepers, M.H.P.C. Chaves, K.S. Jessen, "Spamming chains: a new way of understanding spammer behavior", The 6th g Conference on Email and Anti-Spam, 2009.

[14] C.A. Shue, M. Gupta, J.J. Lubia, C.H. Kong, A. Yuksel, "Spamology: a study of spam origins", The 6th Conference on Email and Anti-Spam, 2009.

[15] A. Cournane, R. Hunt, "An analysis of the tools used for the generation and prevention of spam", Computers and Security, Vol. 23, pp. 154–166, 2004.

[16] D. Boneh, "The difficulties of tracing spam email". Technical report, Department of Computer Science, Stanford University, available at http://ftc.gov/reports/rewardsys/expertrpt_boneh.pdf, 2004.

[17] E. Harris, "The next step in the spam control war: Greylisting", White Paper, available at http://projects.puremagic.com/greylisting/whitepaper.html, 2003.

[18] Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, IETF Documents, available at http://tools.ietf.org/html/rfc575, 2010.

[19] OpenPGP Message Format, IETF Documents, available at http://tools.ietf.org/html/rfc4880, 2007.

[20] Certified Server Validation (CSV), IETF Documents, available at http://tools.ietf.org/id/draft-ietf-marid-csv-intro-02.txt, 2005.

[21] Sender ID: Authenticating E-Mail, IETF Documents, available at http://tools.ietf.org/html/rfc4406, 2006.

[22] P. Ostrihon, R. Rajabiun, "The robustness of new email identification standards", COMDOM Software and York University, White Paper, available at http://www.virusbtn.com/pdf/conference_slides/2008/Ostrihon-Rajabiun-VB2008.pdf, 2008.

[23] Simple Mail Transfer Protocol, IETF Documents, available at http://tools.ietf.org/html/rfc5321, 2008.

[24] İstenmeyen Posta (Spam) Önleme Pilot Çalışma Sonuçları, available at http://www.ttnet.com.tr/i/assets/docs/spam_pilot_calisma_sunumu_27mayis.pdf, 2009.

[25] The Domain Block Lists, Spamhaus Inc., available at http://www.spamhaus.org/dbl/, 2012.

[26] The Apache SpamAssassin Project, Apache Inc., available at http://spamassassin.apache.org/.

[27] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, J. Barker, "Detecting spam zombies by monitoring outgoing messages", The 28th IEEE Conference on Computer Communications, pp. 1764–1772, 2009.

[28] Open Source, Free, Community-Supported Security Solution, Endian Inc., available at http://www.endian.com.

[29] Postfix Project, available at http://www.postfix.org.