The Second International Conference "Problems of Cybernetics and Informatics" September 10-12, 2008, Baku, Azerbaijan. Section #1 "Information and Communication Technologies" www.pci2008.science.az/1/23.pdf

NEW ANTI SPAM METHODS

Saadat Nazirova

Institute of Information Technology of ANAS, Baku, Azerbaijan, *saadatn@mail.ru*

Introduction. Ideal anti-spam solution should not make wrong filtering and be capable to identify 99.9% of spam messages in most cases. We use phrase «In most cases», because it's almost impossible to succeed in both tasks at a time. Not only identification of 100% of spam messages is important but avoiding wrong identification, the case when legitimate message is identified as spam is also crucial. Existing anti-spam products can filter out incoming and outgoing correspondence at quite satisfactory level and appropriately label them allowing minimum 2-3% of wrong identification. Though a lot of effort has been put in this direction [1-4] existing products still cannot completely avoid wrong identification. Therefore final manual filtering is done by end user in order to avoid the situation when legitimate correspondence is identified as spam or manually mark as spam the message which has bypassed the filters and entered the Inbox. Sometimes it's almost impossible visually identify legitimate message among hundreds of spam.

The methods offered in this article allow to significantly increase the overall spam filtering quality.

1st Method: Iteration Filtration of unread correspondence upon anti-spam definitions base update. It is considered to perform re-scanning of unread correspondence after each update operation of anti-spam definitions. In case when wrong identification has been detected (false positives, true negatives) the appropriate alert should notify about an action, that system should take (i.e. Move unread message to Spam folder or move legitimate message to Inbox folder). In case when user doesn't respond then after certain timeout system should move detected messages to Quarantine and makes the appropriate log of the operation. Anti-spam activity report reflects all actions that took place during the work which includes: detection of wrong identification cases, information about the quarantine folder, number of messages and disk space used.

Even simple incoming mail filtering operation could slow down the performance of end users computers, especially when there is a demand on scan of old unread correspondence.

Unread correspondence can be divided in two logical groups: pre existing unread correspondence, before send/receive operation and newly arrived unread correspondence, after send-receive operation. Monitoring and scanning process should not take too much of system resources, otherwise the spam solution will prevent the end-user from effectively using its computer. On the other hand we still cannot turn off old anti-spam definitions from database, because it could lead to new spam attack from old spam sources or tools. Therefore proper utilization of system resources is very important task. Anti-spam monitoring should be seamless and not affect the performance of primary tasks but on the other hand should provide strong protection against spam. Provided method includes the ability to define which spam filter lists will be used and select the target area, as certain folders or group of unread message that could be excluded from spam monitoring cycles.

2nd Method: Flexible Correspondence Sorting «Not spam/Fresh accounts/Suspicious/Spam". Usually anti-spam tools use strict filtering in two categories «spam/not spam». However, as have shown the researches lead by the author, there are formed 4 groups at recognition of a spam:

1. Exactly non-spam
2. More likely non-spam, than spam
3. More likely spam, than non-spam

4. Exactly spam

First target group is the correspondence, received from addresses which took part in mail discussion with recipient, or from addresses included in recipient's white list (trusted addresses list).

Second group consists of addresses that sent mail to recipient for the first time. These addresses are in risk group, because as usual these addresses are the source of spam messages bypassing anti-spam filtering technologies. Usually these are the addresses and contents of messages which are not yet including in spam definitions files of spam filters.

The correspondence which is sent from the providers brought in black lists, because of mass dispatches of a spam from networks served by them, usually belongs to the third group. This is not yet the fact of that the sent mail is a spam, but allows to assert that this correspondence can be undesirable with the high probability.

Forth group is 99-100% spam.

Traditional anti-spam ttechnologies plase the first two groups of correspondence ("Exactly non-spam" and "More likely non-spam, than spam") into Inbox folder. Thereby does not exclude a contamination of mail box with spam. The third and fourth group of the correspondence ("More likely spam, than non-spam" and "Exactly spam") are plases into Spam folder. Thereby the valuable correspondence for the recipient loses in spam.

Replacement of Non-spam/Spam hard sorting to flexible Non-Spam/Newbie/Doubtful/Spam and distribution of the correspondence on four "Non-Spam", "Newbie", "Doubtful" and "Spam" folders will significantly raise adequacy of a filtration. It is possible to block all mails of 4-th group for a while at excess of threshold value of receipt spam correspondence.

3rd *Method: Anti-spam filter for outgoing correspondence check.* This method assumes that anti-spam module will be applied on Internet Service Provider side. Anti-spam module which makes outgoing correspondence filtering consists of two components: Detection module and Application module. Detection module is being triggered in first place. First module checks the following 3 cases step by step:

1. comparison of outgoing message count M_{ip} from certain IP address IP within certain period of time T_{ip} with predefined threshold N_{ip} ;
2. comparison of outgoing message count M_H with duplicate headers ***H*** within the predefined period of time T_H and predefined threshold N_H ;
3. comparison of outgoing message count M_B with duplicate message bodies ***B*** withing the predefined period of time T_B and predefined threshold N_B .

The Application module will work after detection of a belonging to spammer of this or that address. Application module defines which packages will be transmitted and which will de declined. The Detection module will limit a passband of those packages for which takes place, at least, one of the following conditions:

$$M_{ip} >= N_{ip} ,$$
$$M_H >= N_H ,$$
$$M_B >= N_B ,$$

The parameter of throughput is inversely proportional to, M_{ip} , M_H and M_B Restriction can be carried out with the help of means accessible at the level of gateway screens and batch filters of the modern realizations of *nix (Linux, UNIX) servers [5, 6].

After reaching the appropriate threshold M_{ip} , M_H , M_B system administrator sends notification mail to end-user with activation code in order to predict if the end-user is a living person or bot. In case of failed authorization Internet Service Provider block the user or account

4th *Method: Senders reliability assessment.* It is offered the new filtering module for the existing anti-spam products to achieve the best results in spam estimation and to not allow the loss of the authorized correspondence along with spam. The filtering is conducted on the basis of age of the mail account of the sender.

But before that SMTP protocol must be extended which will allow to include account history in HELO (changes will be applied in order to keep backward compatibility with old version). Mail service providers should support the new protocol, in order to make possible account age check.

At present this parameter is not displayed in the existing protocole [8]. It is offered to add a new command 250- into SMTP protocole. If for a post server the mail is stored by Internet provider, then with the help of this command it is possible to receive age of the mail account of the mail sender and to conduct a filtration using this parameter. The offered method is considered in detail at the paper [9].

Results. The considered methods can be realized alongside with the traditional anti-spam technologies. It is necessary to note that the development and acceptance of the international standard, about expansion of SMTP is necessary for the realization of a fourth method.

It is necessary to struggle with spam not only technically, but also legally. The problems connected to potential opportunities and mechanisms of struggle of the state authorities with undesirable correspondence are considered in the works [10, 11].

Literature

1. Vipul V.P., Adam O. Fighting spam with reputation systems. // ACM QUEUE. November 2005. pp. 37-41.
2. Shlomo H., Salvatore J.S. Combining email models for false positive reduction. // ACM. 2005, pp. 98-107
3. Joshua G., Gordon V.C., David H. Spam and the outgoing battle for the inbox. // Communications of ACM. February 2007. Vol. 50, No.2, pp 25-33.
4. Le Zhang, Jingbo Zhu, Tianshun Yao. An evaluation of statistical spam filtering techniques. // ACM Transactions 2004, pp. 243-269
5. Tomasz Chmielewski. Bandwidth Limiting HOWTO, www.tldp.org/HOWTO/Bandwidth-Limiting-HOWTO/index.html
6. Jayachandran Maniyeri, Zhishou Zhang, Radhakrishna Pillai.R, A Linux Based Software Router Supporting QoS, Policy Based Control and Mobility. / Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03), 2003, IEEE
7. Nazirova S. A. Anti-Spam module for filtering the outgoing correspondence. // "Transactions of ANAS ", Informatics and control problems. Vol. XXVIII, Baku №3, 2008, pp 158-162, www.science.az/cyber/journal/2008/3-28.pdf
8. SMTP Authentication [Tutorial], 26.03.2008, www.fehcom.de/qmail/smtpauth.html
9. Nazirova S. A. Improvement of Anti-Spam technologies with the help of an estimation of reliability of the sender // PCI 2008, Baku.
10. Alguliyev R. M., Nazirova S. A. Architecture of hierarchical intellectual nation-wide system of struggle against spam. // "INFORMATION TECHNOLOGIES", New Technologies, Moscow, №08, 2006, pp. 32-36.
11. Alguliyev R. M., Nazirova S. A. Mulrilayered multiagent automated system of the filtration of e-mail. // "Telecommunications", Moscow, №07, 2006, pp. 6-10.