ISSN No. 0976-5697

Volume 1, No. 3, Sept-Oct 2010

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

# Critical Analysis of Anti Spam Techniques

Laxmi Ahuja*
Amity Institute of Information Technology
Amity University, UP, INDIA
laxmiahuja@aiit.amity.edu

Dr Ela Kumar
GB University,
Greater Noida, India
Ela_kumar@rediffmail.com

***Abstract:*** Spamming is now considered to be a serious threat to the Internet and a massive drain on financial resources. Cost on fighting with spamming has been estimated for $20 billion each year. Today there are a large number of solutions designed to help eliminate the spam problem. These solutions use different techniques for analyzing email and determining if it is indeed a spam. Spammers designed personalized template emails to deliver their messages and then made use of bulk mailing software for distribution. Present paper discusses various aspects of spamming and critically reviews several anti-spamming techniques in detail.

***Keywords***: Spamming, Filters, Bayesian Algorithm

## I. INTRODUCTION

SPAM – everybody knows it, nobody likes it, and absolutely no one wants it.

The only key to protecting against spam is to empower yourself with knowledge. Know what the typical spam characteristics are, what they look like, and how they would like to bombard you with both financial and computerized danger. To prevent spam, both end users and administrators use various anti-spam techniques. An example of blocking spam includes the use of filters. Despite this, spammers seem to think that if they can get their spam past the filters you are likely to buy from them. This is, of course, a dubious assumption since it seems that those that specifically filter spam are those that are least likely to purchase from the spammer. Nonetheless, spam filtering is essentially an arms race between the spammers and spam filters. Another approach to block spam is of making use of blacklists that contain a list of IP addresses of known spammers or compromised hosts. However, these lists have to be constantly updated because spammers have learned to counteract this by rapidly changing the origin of spam[1]. Some of these techniques have been embedded in products, services and software to ease the burden on users and administrators.

Besides a lot of research and several new proposals, no one technique is a complete solution to the spam problem, and each have trade-offs between incorrectly rejecting legitimate e-mail vs. not rejecting all spam, and the associated costs in time and effort [2]. Present paper surveys several anti-spamming techniques available in literature and evaluate these grounds on one or the other parameters. A critical review on some of spam detection techniques has been analyzed. It also examines the motivation of, and the tools used to generate, spam.

Anti-spam techniques can be broken into four broad categories: those that require actions by individuals, those that can be automated by e-mail administrators, those that can be automated by e-mail senders and those employed by researchers and law enforcement officials.

## II. SPAM BLOCKING TECHNIQUES

Following section discusses various spam blocking technique in detail.

### *A. Word Filters*

Word filters are a simplistic yet effective way to block the majority of obvious spam. Word filters simply identify any email that contains certain key words, such as “bank,” that are commonly found in spam. Because spammers often work to circumvent word filters by purposely misspelling words, word filters need to be regularly updated with variations of the key words. For example, “b@nk” may be purposely misspelled as “ba&k,” so the word filter must be updated to contain both “ba&k” and “b@nk”. In some circumstances, word filters run the risk of creating false positives. For example, a legitimate email containing the word “bank” that is intended for a commercial researcher, finance or bank may be inadvertently blocked. Overall, word filters can be an effective spam blocking technique if they are constantly updated with new key words and phrases, as well as their unique misspellings.

### *B. Rule-based Scoring Systems*

Rule-based scoring systems are a more sophisticated spam blocking technique than word filters. These systems, also known as artificial intelligence (AI) systems, are similar to word filters in that they also check for key words. However, whereas word filters simply just block emails that contain key words, rule-based scoring systems use rules to analyze emails and assign points to each key word it finds. For example, an email that contains the word “DISCOUNT” in all capital letters might receive +2 points. An email that has the phrase “click here” might receive +1 point. The higher the score, the greater probability the email is spam. If an email reaches a certain score or threshold, it is then classified as spam. Large quantities of spam and legitimate email are used to determine the appropriate scores for each of the rules in rule-based scoring systems [3].

Spam Assassin, an open source spam filter, is an example of a rule-based scoring system. To identify spam, Spam Assassin uses a wide range of heuristic tests on mail headers and body text. Because spammers and their spam-making applications are not static, rule-based scoring systems face some of the same challenges that word filters face. Rules must be updated regularly in order for rule-based scoring systems to

remain effective. For example, if a rule-based scoring system has a rule that assigns points to the word "Bank," spammers can easily circumvent this rule by purposely misspelling "Bank" as many different ways as required to successfully deliver the spam. Rule-based scoring systems, however, if used properly, can be very effective, eliminating over 90 percent of incoming spam.

### *C. Bayesian Filters*

Bayesian filters are very powerful and are regarded as one of the most accurate techniques for blocking spam. Bayesian filtering is based on the principle that most events are dependent and that the probability of an event occurring in the future can be inferred from previous occurrences of that event. This same technique can be used to classify spam [4]. If a piece of text occurs often in spam but not in legitimate mail, then the next time that same text is encountered in a new email, it would be reasonable to assume that this email is probably spam. Most reports on Bayesian filters have shown accuracy of over 99 percent when the filter has been "well-trained." For Bayesian filter training, approximately 200 legitimate emails and 200 spam emails from the intended recipient are normally needed. The more emails in the historical database of the intended recipient, the more accurate the filters are.

### *D. Black List IP*

Black list IP is a common spam blocking technique. It has no computational overhead and is easy to implement. Because spammers regularly change their IP addresses and use a wide range of IP addresses, black lists are most effective in blocking small amounts of spam for short time periods. They provide a quick fix for blocking one particular source of spam but are ineffective as an overall anti-spam solution.

An alternative to a black list is a white list. That is, a list of IP addresses from which you only accept email. This reverse concept of black lists, however, is impractical because users would only be able to receive email from IP addresses that they knew beforehand, making it impossible to receive email from any new sources.

### *E. RBLs (Realtime Blackhole Lists)*

RBLs (Realtime Blackhole List), also known as DNSRBLs, check every incoming email's IP address against a list of IP addresses in the RBL. If the IP address is part of the RBL, then the email is identified as spam and blocked. Unlike the black list IP technique, RBLs are not manually updated by organizations. RBL operators maintain public RBLs and organizations simply subscribe to them. Many organizations like using RBLs because they not only have low computational overhead but because they are normally implemented using a protocol similar to DNS (Domain Name Server), they also have low network overhead.

A downside of RBLs is that they may generate false positives. Most RBLs are aggressive and block all reported spam sources. However, many times the spam sources, such as popular ISPs Yahoo, Earthlink or Hotmail, are also the source of legitimate email. In those cases, the legitimate email is typically never received since it is rejected as soon as its IP address is identified. The RBLs can not differentiate between when a source is sending spam and when it is sending legitimate email. It just blocks any email coming from the IP addresses in its list, thereby generating false positives at times. RBLs are effective for blocking spam and should be part of an organization's spam blocking strategy. With careful selection of which RBLs to use, you can effectively eliminate spam without the downside of generating false positives [3].

### *F. DNS MX Record Lookup*

This is an effective technique for blocking spam from spammers who use a fake from and/or return address. Spammers use such fake addresses so that the spam cannot be traced back to them. To determine if a from address is valid, the system does a lookup on the domain that is used in the from address. If the domain does not have a valid DNS MX record, then the address is not valid and that email is labeled as spam. Similar lookups can be performed on the return address of the email as well.

### *G. Reverse DNS Lookups*

This is an effective spam blocking technique that uses a reverse DNS lookup on the incoming email's source IP address. If the domain provided by the reverse lookup matches the from address on the email, the email is accepted. If they do not match, the email is rejected.

Reverse DNS lookups, while popular, often do not work well. They can generate a large number of false positives since many reverse DNS entries are not properly established and many more cannot be properly established. For example, any "vanity" domain name would most likely not have an accurate reverse DNS lookup. As such, emails from these domains would be rejected, causing unacceptably high false positive rates [7].

### *H. Black List Sender Email Addresses*

This is a simple spam blocking technique that is often used. Users create a black list of from addresses that should be prevented from entering the network and reaching the user's inbox. There are a few disadvantages with using this technique. Because spammers can create many false from email addresses, it is difficult to maintain a black list that is always updated with the correct emails to block. Also, some spammers do not even use a from address so a black list would not be able to catch these cases. Even a rule to block emails without a from address would not be sufficient because some legitimate emails, such as newsletters to which a user may subscribe, may also not include a from address. Black list sender email addresses is effective in temporarily blocking a small amount of spam but ineffective as an overall anti-spam solution.

As an alternative to black lists, some users set up an email white list consisting of acceptable email addresses or domains. In this case, users only accept email from users that are listed on their white list, while all other email is blocked. This technique poses many challenges as well since people want to be able to receive email from people that they might not have entered into their white list.

Some techniques will attempt to automatically build the white list from email that you have sent or from your address book. This makes creating the list easier. However, it does not solve the problems associated when people who legitimately want to send you email have not previously corresponded with you via email, have multiple email addresses, or have a new email address.

### *I. challenge/Response Systems*

Challenge/response systems are used to counter spammers who use automated mailing programs to generate millions of

 

spam emails per day. These systems are designed to slow down spammers by putting roadblocks up for the incoming spam.
Challenge/response systems, such as those offered by Spam Arrest or MailBlocks, maintain a list of permitted senders. Each time an email from a new sender is sent to a challenge/response system user, the email is temporarily held before delivery. The challenge/response system sends the email sender a challenge. This challenge usually consists of a link to a URL or a request that the sender copy a numeric code into a box in the reply email. If the sender successfully completes the "challenge," the challenge/response system adds him to the list of permitted senders and his email is delivered to the intended destination.

### *J. Computational Challenge Systems*

Computational challenge systems add a cost to sending email by requiring the sender's system to perform a computation prior to sending the email. Most computational challenge systems use complex algorithms that are intended to take time to process. The hope is that a high enough cost would stop people from sending spam to those with computational challenge systems. How do computational challenge systems work in practice? Let's assume Derek is using a computational challenge system to help stop spam. A new friend, Joe, decides to send Derek an email for the first time and therefore is not yet on Derek's list of acceptable senders. Derek's server receives the email and sends a computational challenge (typically a math problem or algorithm) to Joe's email client. Derek's server waits for a response before allowing the email to be delivered to Derek's inbox.

### *K. Rate Controls*

Sometimes spammers attempt to cripple email servers by sending a large quantity of email in a short period of time. This is called a DOS (Denial of Service) attack. With rate controls, a system administrator can set up parameters that protect the email server from this email flood. Rate controls can be set up to allow only a certain number of connections from the same IP address during a specified time. For example, a rate control time can be set to 30 minutes with only a certain number of connections to be allowed in that given time period. If the administrator sets this parameter to 50 connections, the firewall will block any correspondence after the first 50 connections that come from a single IP address within a given 30 minute time period. Rate controls are effective in protecting the network from spammers who attempt to send hundreds of spam emails at the same time to a specific email server.

### *L. Machine Learning*

Spam filtering based on the textual content of email messages can be seen as a special case of text categorization, with the categories being spam and non-spam. Although the task of text categorization has been researched extensively, its particular application to email data and detection of spam specifically is relatively recent. Although high performance levels were achieved using word features only, it was observed that by additionally incorporating non-textual features and some domain knowledge, the filtering performance could be improved significantly [8].

### *M. PageRank Algorith*

The citation (link) graph of the web is an important resource that has largely gone unused in existing web search engines. PageRank is an excellent way to prioritize the results of web keyword searches. For most popular subjects, a simple text matching search that is restricted to web page titles performs admirably when PageRank prioritizes the results [9].

### *N. Anti-Virus Scanning*

Anti-virus scanning can really be viewed as a method of stopping spam since a large amount of unwanted email is generated by virus programs that attempt to propagate themselves. A virus scanning solution is certainly an effective tool to include as part of any organization's overall anti-spam solution.

## III. EXAMPLES OF ANTI SPAMMING TECHNIQUES

Message Sniffer (SNF) is an intelligent anti-spam scanner that uses advanced pattern recognition and collaborative learning technologies to accurately identify spam, scams, viruses, and other email borne malware at your email server or gateway (before it gets to your inbox). SNF accurately captures more than 99% of spam without tuning. This is not "market-speak". We calculate this statistic from real-world data collected by our monitoring system using system telemetry, data from spam-traps, user submissions and a comparative analysis with several dozen high quality spam tests.
In addition Message Sniffer's highly optimized engine has very modest hardware requirements and typically uses only a small fraction of the resources required by other engines (SNF typically has less than 10% of the CPU requirement of SpamAssassin when processing the same message stream!) [10]
Heuristic approaches attempt to detect certain text patterns in e-mails that may permit them to be classified as spam or non-spam. CORE is a statistical process that classifies e-mails according to their content. It is based on Support Vector Machines, one of the highest-performing algorithms for text analysis. Pornographic e-mails are blocked using the Xblock image analysis function.[4]
*SpamArrest***:** SpamArrest combines a webmail and spam filtering solution for ease-of-use. It offers portability and can also be easily integrated with current email software.
*Qurb***:** This is another affordable and effective spam blocking program that integrates Outlook or Outlook Express setup. Internationally recognized as a superior solution for stopping spam dead in its tracks, Qurb is a great antispam solution.
*Mailwasher Pro*: Mailwasher Pro is a simple, effective solution to spam that doesn't depend on having Outlook or Outlook Express installed. For scanning email before it ever arrives on PC then Mailwasher Pro may be a good solution. Most other spam blockers first have to download the mail to your PC before doing anything. Mailwasher Pro allows to preview incoming mails and delete or bounce the ones, you don't want to receive.

## IV. HOW TO PROTECT SPAM

Various methods are combined to produce an efficient and powerful defense against spam. The following sequence has proven effective in practice for e-mail analysis:
Check address using blacklists (prohibited e-mail addresses and domains) and company specific white lists (permitted addresses and domains). The white lists contain business relevant sender addresses, e.g. for customers, suppliers, newsletters, discussion forums.
Check subject line for simple keywords using dictionary (100%

 

stop words).
Check message text using dictionary and HTML analysis. In this step, the dictionaries
used should contain 100% stop words, similar to the dictionary for the subject line, in order to immediately sort out corresponding e-mails as spam. Dictionaries with 100% stop words are generally shorter and require less maintenance.

*Check e-mail content with CORE:* Without CORE, a user can eliminate no more than 73% of spam – and this is a declining trend, because new spammer tricks can circumvent these static methods. With CORE, however, a user can detect 97% of incoming spam e-mail now and in the future, because CORE is an adaptive technique and learns to recognize new spammer techniques as they appear.

## V. CONCLUSION

Spam is a problem that is continuing to grow from day to day, costing corporations billions of dollars in lost productivity. Fortunately though, there are different spams blocking techniques to help counter the various types of spam. Because spammers are always trying to bypass anti-spam techniques by changing the methods they use to send spam, it's best for corporations to protect themselves with a spam blocking solution that uses more than one spam blocking technique. Each one of these techniques has advantages, disadvantages, as well as limitations. To minimize the amount of spam that enters an organization, a spam blocking solution that includes a combination of the most effective techniques should be implemented.

## VI. REFERENCES

[1] McAfee Anti-Spam: Protecting Your Organization from Spam, Phishing, and Other Unsolicited Messages (2006) , available at http://www.mcafee.com/us/local _content/white_papers/anti_spam.pdf

[2] Anti Spam Techniques, available at http://en.wikipedia.org/w/index.php?title=Anti-spam_techniqueswww.gfi.com

[3] An Overview of Spam Blocking Techniques, available at http://www.gcr.com.hk/Whitepapers/ Barracu-da_Spam_Techniques.pdf

[4] Bayseian Approach, available at http://www. news/en/gfi.com/ mes9bayeswp.htm

[5] Message Sniffer at http://www.armresearch.com/products/index.jsp?gclid = CPLP_O-Z4CFYowpAodFkqEIA

[6] Anti-Spam & Anti-Phishing, available at http://www.group-technologies.com/en/products/solutions/antispam.php

[7] Barracuda Networks, available at www.barracudanetworks.com

[8] Md. Rafiqul Islam, Morshed U. Chowdhury, Spam Filtering Using Ml Algorithms, IADIS International Conference on WWW/Internet 2005, pp: 419-426.

[9] Sergey Brin and Lawrence Page, The Anatomy of a Large-Scale Hypertextual Web Search Engine, available at http://infolab.stanford.edu/~backrub/google.html.

[10] Message Sniffer Anti Spam Filter - High Performance Scanner available at http://www.armresearch.com/products/index.jsp

 