GATEWAY ABSTRACTION FOR FOOLING THE SPAMMERS

Mrs.N.Nagadeepa M.Sc.,M.C.A.,Mphil.
Lecturer in Computer Science,
Vivekanandha College of Arts and Sciences for Women,
Tiruchengode (Namakkal).
(Research Scholar)

ABSTRACT

Unsolicited commercial email or "spam" flood mailboxes, causing frustration, wasting bandwidth, and exposing minors to unsuitable content. This paper uses intelligent gatekeepers to interact with spam messages and system referenced in spam. The goal of this paper is to consume spam senders' resources by engaging the spammer in appropriate gatekeepers. There are four gatekeepers have been implemented: Phishing gatekeeper, medicine gatekeeper, bank scam gatekeeper, and web form gatekeeper. This technique provides better results and it cannot deal with the image spam.

Keywords- spam, Phishing gatekeeper, medicine gatekeeper, bank scam gatekeeper, and web form gatekeeper.

1. INTRODUCTION

The primary reasons of the spam are profitable and low cost, with respect to both computing and human labor. This paper began as a technique, refer to as gateway. It attacks the senders of spam. The basic idea of this technique is to pose as a dupe by responding to spam, forcing spammers to spend time pursuing a false lead or dupe.

The idea of this paper is that spam could be greatly reduced if we could encourage the public to have a different sociological response to spam. Spamming schemes such as bank scam, phishing, medicine advertisement and web forms become ineffective if spammers are flooded with dupes. But it is not realistic to rely on a change in human behavior to bring this idea forward. So this technique has now shifted creating an artificial intelligence gateway to carryout this behavior. It is an intelligent gateway paradigm whose sole purpose is to consume as much of the spammers' resources as possible. For spam that makes it through a spam filter, rather than clicking junk button, a mail user can click a gateway button on the users' mail toolbar. The gateway has four spam gate keepers: Phishing gatekeeper, medicine gatekeeper, bank scam gatekeeper, and web form gatekeeper.

2. STATEMENT OF THE PROBLEM

The increasing popularity and low cost of email have intrigued direct marketers to flood the mail boxes of thousands of users with unsolicited messages, advertising anything from vacations, to get-rich schemes. These messages known as spam or more formally unsolicited commercial email. Those are extremely annoying, as they clutter mailboxes, prolong dial-up connections, and often expose minors to unsuitable content.

3. OVERVIEW OF SPAM

In this paper spam is defined as unsolicited commercial mail [9]. It is necessary to point out that some people want to receive these messages. There is an audience for email advertising, regardless of the product that is being sold. Spammers are trying to reach these people. Spammers do not know which people comprise this group. To reach them, they send spam to as many people as possible. This is cone because they don't know who will respond to the message and who will not.

Spammers are generally technically skilled individuals that are hired by companies to send spam. By using a third party, the companies try to keep themselves from getting sued [13]. For a company spamming can be very uncreative if done right. For example a company is selling monkey dolls for 50 dollars a doll. If the company lets the spammer send out 10 million mails and the response rate is just 0.1% it will make half a million dollars [5].

Spammers get email addresses by forging them from websites, newsgroups etc [5]. It is possible to turn this into an advantage, by fooling spammers with fake email addresses and thus harvesting their spam.

4. RELATED WORK

The spam gateway built upon work used to classify different types of emails. Much work has been done in classifying spam versus non-spam email. Trudeau et al. [11] overviews different techniques of classifying email. Carvalho et al. [2] classify emails as a speech act, such as a request or question. Another similar concept put forth by Martine et al. [7] is to classify emails based on behavioral features using statistical learning. Likewise Drdze et al. [3] uses an algorithm to classify emails into activities. The gateway

system relies on classification not only to determine spam versus non-spam, but also to classify the type of spam to select an appropriate gatekeeper.

Oudet [8] suggests creating a "honeypot" of fake proxy as a way to detect, slow, and block spammers. Goodman et al. [4] advocate that the best way to reduce spam is to add a cost to sending emails. They believe that adding a Turing test every X amount of emails would require the spammer to spend time proving that it was human. This lessens the capability and feasibility of using an automated way to spam. Another aspect of the paper also advocates adding a cost to sending an email. There could be an actual monetary cost or there could be a computational cost. Johansson et al. [6] have developed a system called CAMRAM to do exactly that. Blue security [10] attempts to consume spamming resources by having all users of its software automatically and repeatedly send out messages to spammers and their ISPs. This approach differs from the most of the methods in that these are directly targeting the consumption of human spamming resources rather than machine resources, and the penalty occurs after the spam has been sent.

5. CONCEPTS OF SPAM FILTERING TECHNIQUES

5.1 Blacklist

Blacklists like the MAPS realtime backhole list (9) are the oldest approach to filter spam messages. A central list, usually managed and altered by an operator, is used to store information about the address of mail servers sending spam. Especially ISPs, hosting mail accounts for many users, used to apply this filter technique and simply blocked all messages coming from a server listed on such a blacklist.

Advantages

The main advantage of blacklists in that they do not only stop a current spam messages but also every future spam from the same server. Spammers are there-fore forced to change the IP addresses of their servers regularly and cannot continuously send spam from the same server over longer periods.

Disadvantages

Blacklists have a lot of disadvantages and only the worst ones are presented here. The worst problem about blacklists is that they produce a lot of false positives. Since spammers often use hacked or open mail servers to send their advertisements, these abused servers can get blacklisted. As a result, the good mails sent over these servers will get blocked as well by any ISP using the blacklist. A study from 2001 claims that the MAPS RBL has a false positive rate of more than 30%, which is absolutely unacceptable. Since blacklists only stop spam from known servers, they miss a lot of unwanted messages, because the sending servers may not be known yet. The study mentioned above also reports a spam detection rate of less than 25% for the MAPS Also, the users of a blacklist usually do not have a chance to influence which servers are blacklisted but have to trust the list owner. In the past, several scandals became public where blacklist which never sent out any spam but belonged to someone who fell in disgrace with the list owner.

5.2 Rule Based Filter

Rule based filters like the widespread Spamassassin [10] system analyze the content of an incoming message according to a given set of filter rules. Header, subject and body of the mail are parsed and spam probability is calculated depending on how many spam rules match.

Advantages

Rule based filters are very versatile and can be used directly on the mail server or the client side. Since the efficiency of these filters heavily depends on the quality of the rule set used, a centralized system has the advantage that one administrator can keep the system up to date for all users. A client side installation offers more flexibility though, since each user may set up individual rules.

Disadvantages

Since Spam messages are constantly adapted to pass as many filters as possible, it is necessary to keep the filter rules up to date. Especially novice users may find this task difficult and can be forced to rely on external sources to get new rule sets. Another problem is that rule based filters tend to block mails with exotic text layouts. For example, most of these filters have a rule that marks a message as spam if it contains too may words in capital letters. While in most of the cases a mail triggering this rule really is spam, there are also innocent messages that of false positives, a rule based system usually requires a mail to match several conditions before it gets marked as spam. The perfect tradeoff between filter efficiency and minimum amount of false positives is hard to fine and needs constant adaptation of the system

5.3 Bayesian Filter

Bayesian filters are a sub-species of rule based filters and are currently often named as the best spam filters available. Bayesian filters do not use a static set of rules to identify

spam but rely on dynamically generated token lists. A token can be anything from a letter to whole phrases, depending on the algorithm used. The filter keeps two lists: one for good tokens seen in normal mails, and one for bad tokens, which appear in spam messages frequently. Every incoming message is parsed and the tokens it contains extracted. The filter then decides depending on the good to bad token ratio found, if the message is spam or not. Due to the high popularity of this approach there are a lot of different implementations for various mail clients and operating systems available. Paul Graham, one of the leading heads in bayesian filter development, maintains a very informative website (11) where most of the working filters are linked.

Advantages

One of the best things about bayesian filters is that they do not need to be configured but learn from the user's behavior. If the user removes a message the filter identifies the important tokens within the mail and adds them to the bad tokens list. After a short time, this list contains most of the suspicious tokens and incoming spam is detected at a high rate.

Good mails, which are not removed as spam, are also parsed and the detected tokens are added to the good tokens list. This list is responsible for the low rate of false positives bayesian filters are known for. A mail containing several good tokens will not be marked as spam, even if there are some bad tokens present. Since the token lists are compiled individually, the filter adapts to the user's environment, allowing an employee of a bank to receive mails containing text about loans and credits while the same messages are rated with a high spam probability if they are received by another user.

Disadvantages

One weak point of the bayesian filters is their need to identify tokens within a mail, since the spammers can use various techniques to cloak their messages. The simplest way to do so is to misspell suspicious words or to insert additional characters. For example, the classic amongst the spam words "sex" can also appear as "sex" or "s.e.x". If the message is encoded as HTML, there are even more ways to confuse the filter. For example HTML comments may be inserted, which are not visible to the user but to the filter. While the user sees "free cash" the HTML code may look like this:

fr<!—com1 -->ee c<!—com2 -->as<!—com3-->h

While it is possible to deal with simple attacks like these there are ways to write a message which leave no tokens detectable. Figure 1 shows an easy example how an HTML table and a mono spaced font may be used to write an undetectable spam message. An HTML table with one row and invisible borders is generated. The corresponding letters of each line are put together in one table field and html line breaks
 are used to split them up again. While the user sees the text as usual from the left to the right, the characters appear top down in the HTML code. Even a good parser will have trouble to decode this kind of message correctly.

Another weakness is very short mails which only contain a line to an image with the advertisement. The bayesian filters completely fail here, since these messages do not contain any useful tokens at all. Finally, the spammers may also abuse the good tokens list to make their messages look better, the names of friends and business partners become good tokens, since they appear in good mails frequently. Therefore, the spammers have started to add hundreds of names to their mails hoping to include at least some of the names the receiver has on the good tokens list. In certain environment, like the banking business mentioned before, this effect may even lead to problems without any modification of the spam message. The terms "credit" and "loan" are surely on the good tokens list of a bank employee for obvious reasons. As a result, the spam mails concerning financial topics will not be filtered for these users.

THIS IS A
TEST MESSAGE

T	H	I	S		I	S		A			
T	E	S	T		M	E	S	S	A	G	E

Figure 1.Table with one column and HTML line breaks to separate the characters in the cells. The resulting HTML code does not contain any readable strings and is hard to parse.

5.4 Collaborative Filter

Collaborative filter do not try to identify spam mails automatically but rely on user feedback. The main idea is to connect a large number of users who all report their spam mails to a well known hub. This central entity generates an identifier for each reported message (based on its content) and stores this so called "fingerprint" for later lookups. Whenever a cline receives a mail, the corresponding identifier of that message is calculated and compared to the central list of known spams. If the message has already been reported by any

user, its identifier will be found on the list and the mail will be marked as spam.

<table><tr>
<td>T
T</td><td>H
E</td>
<td>I
S</td><td>S
T</td>
<td>
&nsbsp;</td>
<td>I
M</td><td>S
E</td>
<td>
S</td>
<td>A
S</td><td>
A</td>
<td>
G</td><td>
E</td>
</tr></table>

Advantages

The clear advantage of collaborative spam filters lies in the fact that they use the best spam detector possible the human user himself. If there are enough users cooperating, the individual participant does not have to report a lot of messages any more, since only the first few recipients of a new spam mail need to report it and all other receivers will have the message removed automatically. Also, the risk of false positives is low, since they only happen if malicious users wrongly report a good message. Complex trust systems can be used to reduce the rate of false positives by malicious users even further, creating the probably most efficient spam filter concept available.

Disadvantages

The efficiency of collaborative spam filter tools directly depends on the quality of the fingerprints generated for the reported messages. It has a long time since the spammers have started to include randomized land personalized parts in their mails, which look different for every recipient. Therefore, it is difficult to calculated and accurate identifier for a message that also matches a slightly different looking version of the same mail received by another user. Collaborative systems also have to deal with malicious users reporting good mails as spam. While it does not matter if an individual message is reported as spam (since it is fingerprint will match any other mail) a reported newsletter leads to problems. Therefore, most collaborative systems offer a client side whitelist which allows the user to stop the system from checking certain mails. While these whitelists work pretty well in most of the cases, they still have to be seen as a workaround and not as a solution to the problem.

6. METHODOLOGY

6.1. Gateway

The gateway architecture is shown in figure1. It is used in conjunction with a traditional spam filter. When an email comes in it is either classified as spam or normal email by the email client's spam filter. The spam then can be deleted from the system or to be passed to gateway. Sometimes spam gets past the filter. This is called false negative in that case the user may pass the spam directly to gateway.

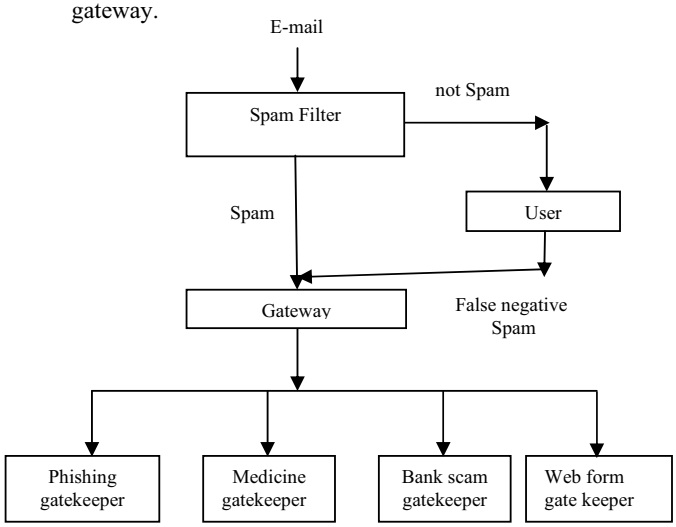

Figure 2. Normal Email

The next step is for the gateway to decide which gatekeeper to have handle the spam. If the spam is classified as bank scam, then it is passed along to bank scam gatekeeper. If the spam is classified as web spam, then it is passed along to web form gatekeeper. If the spam is classified as phishing, then it is passed along to phishing gatekeeper. If the spam is classified as medicine advertisement, then it is passed along to medicine gatekeeper.

6.2. Phishing gatekeeper

Phishing gatekeeper is targeted to phishing spammers. The initial phishing gatekeeper strategy will be to flood the phishing with long and complex user names and passwords. The result will be something close to a denial of service and will fill the phishing database with massive amount of false usernames and passwords.

6.3. Medicine gatekeeper

Medicine gatekeeper is designed to response the medicine advertisements. The medicine gatekeeper database includes the medicine messages like what is the offer?, how it is possible, contact me, send medicine details etc., when a message received from the spammer, the above response messages are sent by the gatekeeper.

6.4. Bank scam gatekeeper

The bank scam gatekeeper is designed to interact with the bank scam spammers if a real person is responding to the spam. In order to do so, the gatekeeper first parses the email.

The initial spam mail has most of the information needed to get a conversation started. To identify the spammer the gateway will use the spam keywords, which are previously sent by the spammer. The keywords are stored in a database. The gateway compares the words in a spam message with the keywords in database. Then it decides the spam message belongs to which gatekeeper, and then the spam is passed to appropriate gatekeeper. Next gatekeeper response is sent to the spammer. Gatekeeper responses are stored in a database and are stored by categories such as: who are you, I am interested money issue, send your phone number etc,. There are multiple messages per category type. The agent tracks what type of response categories it has sent out to limit duplicate messages. Bank scam gatekeeper will continue to return messages to the spammer as long as spammers keep replying.

6.5. Web form gatekeeper

Web form gatekeeper is designed to fill out spam web forms of the sort received from mortgage brokers and online universities. These forms request information to pursuer a future sale. As with bank scam gatekeeper, the purpose of the web form gatekeeper is to receive a response from the spammer. After following the links to a form, web form gatekeeper will parse the form to generate inputs. The form will be filled out to maximize interest from the spammers. This gatekeeper also have setup email database to track spammer interactions.

7. CONCLUSION

This approach is novel and shows promise. This approach is complementary to existing filtering techniques, giving mail users the option of employing gatekeeper on spam messages that makes it through their server or client filters. A more suggestive strategy would be to also apply gateway gatekeepers to automatically classified spam. In such cases the confidence level that the target is spam would need to be high.

REFERENCES

[1] Anti Spam site, Claws and Paws-http://www.claws-and http://www.claws-and-paws.com/spam-1/tracking.html

[2] Carvalho, Vitor R. and Cohen, William W.On The Collective Classification of Email "Speech Acts". *Special Interest Group on Information Retrieval*. 2005.

[3] Drdze, Mark, Lau, Tessa, and Kushmerick, Nicholas. Automatically Classifying Emails into Activities. *International Conference On Intelligent User Interfaces*. 2006.

[4] Goodman, Joshua and Rounthwaite, Robert. Stopping Outgoing Spam. *ACM Conference on Electronic Commerce '04.* 2004.

[5] Internet Privacy for dummies-http://www.internetprivacyfordummies.com/modules.php?op=modlod&name=sections&files=index&req=listarticlessecid=3

[6] Johansson, E.S.CAMRAM. Available at http://www.camram.org.

[7] Martin, Steve, Sewani, Anil, Nelson, Blaine, Chen, Karl, and Joseph, Anthony D. Analyzing Behavior Features for Email Classification. *Conference on Email and ante-Spam.* 2005.

[8] Outdet, Leurent. Fighting Spam With Honeypots. November 26, 2003. http://www.securityfocus.com/infocus/1747.

[9] PC World Spam news-http://www.pcworld.com/resource/spamwatch.asp

[10] Spring, Top. Bringing Spammers to Their Kness. *PC world.* July 18, 2005. http://www.pcworld.com/news/article/0.aid.121841.00.asp

[11] Trudeau, Paris, Cullen, Richard, and Zwieback, Dave. Major Techniques for classifying Spam. *SurfContro*l, 2003.

[12] UNX Spam combat organization-http://combat.unx.com/

[13] Unicom Software Archive: ungoopspam-http://www.unicom.com/sw/nugoopspam/

BIOGRAPHY

Mrs. N. Nagadeepa born on 1978**.** She received her M.Sc., Information Science and Management and M.C.A. degree in 2002 and 2009 respectively from Periyar University, India. She received her M.Phil., degree in 2004 from the Bharathidasan University, Trichy, India. She is having 7.10 years of teaching experience and currently pursuing as a Assistant Professor of Vivekanandha College of Arts and Sciences for Women, Tiruchengodu (Namakkal), India. Her area of interest is Network, Data Mining and Knowledge Discovery.

Her publications are as follows:

- Paper presented at National / International conferences - 6
- Seminars / Workshops / FDP Attended – 5
- Article Publications in Magazines – 3
- Paper Publications is National / International Journals – 2
- Monograms Published – 3