Proceedings of the 2006 IEEE
Workshop on Information Assurance
United States Military Academy, West Point, NY

Quantitative Analysis of Efficient Antispam Techniques

Anders Wiehe, Erik Hjelmås, Stephen D. Wolthusen

Abstract— **While dynamic content-based filtering mechanisms for the identification of unsolicited commercial email (UCE, or more commonly "spam") have proven to be effective, these techniques require considerable computational resources. It is therefore highly desirable to reduce the number of emails that must be subjected to a content-based analysis. In this paper, a number of efficient techniques based on lower protocol level properties are analyzed using a large real-world data set. We show that combinations of several network-based filters can provide a computationally efficient pre-filtering mechanism at acceptable false-positive rates.**

I. Introduction

Unsolicited commercial email (UCE, or "spam") continues to threaten the viability of open electronic mail services on the Internet. While a number of proposals that would close off certain trustworthy user groups by restricting email exchanges to a closed group of email servers or which would require some form of (micro-)payment to ensure delivery, these approaches also can undermine the open interconnection that was instrumental in establishing Internet email [1], [2].

It is therefore necessary – at least in a short and medium term approach – to continue with the deployment and enhancement of techniques for filtering UCE in such a way that the the signal-to-noise ratio remains acceptable to users while keeping misclassifications (i.e. both false positive and false negative classifications) to a minimum despite the continued increase of UCE as a proportion of total message traffic.

However, the problem of UCE volume is twofold: While the primary objective of end users is the reduction of the *relative* amount of UCE (i.e. to maximize the proportion of legitimate emails to UCE), a major concern for system administrators is the absolute volume of UCE and the computational, storage, and bandwidth requirements associated with processing these messages.

While content-based filtering techniques provide very high degrees of accuracy in both selectivity and specificity, their computational complexity requires both considerable resources and can easily become a source of delays or outright failure when overloaded by excessive message traffic. Therefore, it is highly desirable to limit the exposure of content-based filtering mechanisms by imposing a layered filtering architecture using an (computationally) efficient pre-filtering mechanism or combination of such pre-filtering mechanisms.

In this paper, a survey and analysis of filtering techniques based on lower protocol level properties is therefore presented. To this end, section II discusses the experimental setup used in gathering baseline data and also briefly covers the main low-level and content-based filtering approaches. Section III then provides an analysis of filtering sensitivity and selectivity of each low-level technique while section IV subsequently discusses the implications of these results for optimized configuration of filtering mechanisms as well as the limitations of the data set used. Finally, section V provides a brief overview over related work and analyses while section VI describes ongoing and planned research in the area of hybrid anti-spam filtering techniques.

II. Experiment

The results reported here were obtained by providing a transparent filtering mechanism for incoming mail at a small college (Gjøvik University College, Norway) with approximately 1600 students and 130 faculty and academic staff for an extended period. During the 2005 and 2006 period investigated, monthly email traffic was consistently in excess of 300'000 messages. The experiment proceeded in two steps: An initial baseline data collection of messages that were classified by humans as either spam or non-spam and which is assumed to be an oracle function (i.e. the experiment assumes that the human classifier does not make mistakes, at least not at a statistically significant level) for the baseline data set was collected by a filtering configuration which intercepted all inbound message traffic. The baseline data was then compared against the antispam mechanisms under evaluation.

Moreover, the same filter system was subsequently (with one exception, owing to the nature of the antispam mechanism) also used for collecting an additional large number of messages over an extended period of time, which was used to compare the relative effectiveness of individual antispam mechanisms and also of combinations of several mechanisms.

Gjøvik University College, Norway
Gjøvik University College, Norway
Gjøvik University College, Norway and Royal Holloway, University of London, UK

1-4244-0130-5/06/$20.00 ©2006 IEEE

Column name	Possible values
id	unique ID
date	when email first seen
relay_ip	source IP address for email
status_human	spam, non-spam, dont know
status_greylist	spam, non-spam, white-listed
status_spamassassin	decimal number
status_rbl_spamcop	empty, in list
status_rbl_spamhaus	empty, in list
status_rbl_ordb	empty, in list
status_rbl_njabl	empty, in list
status_rbl_sorbs	empty, in list
status_rbl_dsbl_list	empty, in list
status_rbl_dsbl_multihop	empty, in list
status_rbl_dsbl_unconfirmed	empty, in list
status_spf	fail, pass, ...
status_domainkeys	bad, good, ...
status_razor	spam, non-spam
status_dcc	Message count
status_bogofilter	spam, non-spam

TABLE I
Column names and possible values of the result database.

A. Mail Server Filtering Configuration

Given that the data collection was to occur in an operational environment, particular attention had to be paid to ensuring uninterrupted operation. By inserting the experimental mail server between the source network and the regular mail server and forwarding duplicates of messages to the regular mail server, it was possible to meet this requirement (other than under extreme overload conditions where delivery to the regular mail server was delayed).

The experimental server was configured to run the GNU/Linux operating system and the Sendmail MTA (Message Transfer Agent); Sendmail was configured to always queue incoming messages and operate on the queue when server load was low (with the exception of greylisting, see below and section II-C.1). This ensured timely delivery of messages to the regular mail server in real-time and allowed for asynchronous forwarding to filtering modules since this element of the experiment was not time-critical.

Results were collected in a PostgreSQL (an advanced object-relational database management system, also running on the experimental server), see table I for a description of the fields used in this database (the notation "..." indicates values other than spam or non-spam are possible.).

To ensure comparable results for all filtering and countermeasures, all methods were applied on the same mail server configuration. The primary exception to this is the greylisting process, which required timely responses.

B. Baseline Data

To ensure that the automatically collected data sets were calibrated properly and to establish a baseline for the likelihood of a given message being unsolicited commercial email, messages were intercepted and presented to humans for inspection and classification both in 2005 and 2006. The remainder of this paper assumes that these human users can be considered as oracles and do not produce misclassifications.

To this end, volunteers conducted manual classification of 2539 messages, resulting in a total of 1414 messages (or 56%) classified as UCE. For the latest (February 2006) monthly data set, a total of 164546 messages were collected, while the total evaluation is based on a data set consisting of 521010 messages.

The relative performance of the various efficient approaches and the benchmark content-based approaches described in section II-C for baseline data is plotted in figure 3 (circular data points in viewgraph) while the dotted line in figure 3 indicates the (oracle-classified) absolute proportion of UCE of the baseline data.

C. Lower-Level Protocol Antispam Mechanisms

The following briefly discusses the selection of network-based antispam mechanisms that were selected for evaluation and analysis. While several other mechanisms exist, the following selection contains specimens that can frequently be considered typical also for other mechanisms that could not be included in the analysis.

C.1 Greylisting

Greylisting was conceived as a mixture of blacklisting and whitelisting (see also section II-C.4) which can largely be maintained automatically and which does not require excessive human intervention [3]. To be effective, it must be operational on all mail servers for a given domain.

The following three items are used by greylisting:

- The IP address of the host attempting the delivery
- The envelope sender address
- The envelope recipient address

The greylisting approach maintains a database of all such unique 3-tuples it has encountered so far. If a tuple has not been seen, delivery of a message falling under this tuple will be refused with a temporary failure notice at the SMTP level, and the temporary delivery failure will be repeated for messages of the same 3-tuple received within a configurable time window. Since SMTP is a best effort protocol, a conforming SMTP implementation must repeat delivery attempts until either the message has been delivered or a

1-4244-0130-5/06/$20.00 ©2006 IEEE

threshold in the number of attempts or accumulated delay has been reached.

Once a delivery attempt is made outside the greylisting time window, the greylisting database is amended by the 3-tuple as a legitimate communication event and subsequent messages falling under this tuple are accepted and forwarded immediately.

This technique imposes an additional workload on senders by potentially requiring several initial delivery attempts. However, while this cost is amortized over longer message exchanges for legitimate traffic since such message traffic typically exhbits a power-law probability densitiy function [4], [5], this is not the case for senders of UCE. The latter will – unless they have subverted systems running conforming MTA implementations – operate specialized programs that will send messages to legitimate or automatically generated email addresses directly to MX (mail exchange) hosts and relays without accepting replies and therefore also ignoring error messages induced by greylisting.

C.2 Sender Policy Framework

The Sender Policy Framework (originally *Sender Permitted From*) is conceptually based on constraining the set of hosts accepted as mail originators as proposed by Miller in 1998 and is one of several approaches in a family which also includes the Sender ID proposal [6].

Within SPF, the return path of the message is compared with the sender address and checks the IP address of the sender against an SPF record for the domain stored in the DNS (domain name system). Additional extensions can validate several additional header lines using the PRA (Purported Responsible Address) algorithm.

The standardization of proposals in this category has been problematic since unresolved patent claims led to the dissolution of the IETF MARID working group in 2004. Moreover, acceptance of SPF by MX operators has been limited. Given SPF's dependency on widespread adoption of SPF records, this slow adoption significantly affects the overall effectiveness of the scheme.

C.3 DomainKeys / DKIM

DomainKeys has since been re-named Domain Keys Identified Mail (DKIM) and has been submitted to IETF for standardization [7]. In this scheme, the MTA of the sender must sign critical elements (i.e. both several header elements and body) of the message using a public key algorithm, thereby not only ensuring authenticity but also message integrity; the result is then added to the message as an additional header as shown in the example below.

```
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws;
        s=beta; d=gmail.com;
        h=received:message-id:date:from:reply-to:to:
          subject:mime-version:content-type:
          c+ontent-transfer-encoding;
        b=b1FKPFeCr0MO34uurDUwQwIgbkgd9dEpAnKblRw1mx
          fq/l2grBtmpnY50Ue7UW8I0u5Kep31SbWrI+z1z8Lg
          U7YZQyxpf54fY6TSWQA1CJrkh58sTATcdQeY+OXGZL
          hEee04RwtQwY5rV68KHnCOotz59zAZo+u8TgJiBUqD
          2+v4k=
```

All messages must be signed by the sending system, and the public keys for verification of signatures must be distributed to possible recipients. As with SPF, this occurs via an extension to the DNS record system. The DNS must also contain a policy entry for specifying the extent to which DKIM is used by the domain. Recipients can then validate a message by checking that the sending domain signs all outgoing messages and reject any message that is not signed outright. Only in cases where a signature is present is the computation of the message hash value and decryption by the recipient required.

To ensure that some legitimate processing such as forwarding and rewriting that commonly occurs in case of mail reflectors is not affected, these headers are not signed whereas the signed fields are stated explicitly in the DKIM header.

Other approaches in this category are the CLEAR (Compatible Low-Level Email Authentication and Responsibility), CSV (Certified Server Validation), and BATV (Bounce Address Tag Verification); these, however, were not included in the experiment setup.

C.4 Real Time Blacklists

Real Time Black Lists (RBL) provide databases in which hosts are recorded that are considered insecure (e.g. open mail relays or proxies) or are known sources of excessive amounts of UCE. To ensure that these rapidly changing potential sources of UCE are identifiable immediately by an MTA, the the databases are updated in near real-time and also use the low-latency DNS protocol as the transport mechanism for information on blacklisted hosts. For each host from which an MTA receives an inbound email, the RBL must be queried (causing an additional lookup using the DNS protocol). The RBL database may both apply a ruleset in determining to enrol a host in the blacklist and can also indicate the confidence with which the RBL classifies a given host as a source of UCE [8]. If the result from the RBL exceeds a confidence threshold set by the MTA, the message can be discarded.

Since RBL operate at the network level, there is a considerable risk of servers being blacklisted even though only a very limited fraction of the overall users or message traffic is spam. This can lead to severe disruptions, particularly for larger MX operators such as internet service providers. Moreover, the RBL reporting mechanism can result in an indirect denial of service by maliciously reporting a MX host as a source of UCE.

C.5 Razor

The Razor system by Prakash is based on a distributed hash database over the actual content (body) of the email messages processed [9], [10], while a mechanism similar to Razor was also described recently by Deepak and Parameswaran [11]. The rationale behind this approach is that some UCE will be sent out with identical content to a large number of recipients, which can be identified and hence filtered whereas legitimate message traffic will not exhibit congruence with large numbers of messages observed at other sites (with the exception e.g. of mail reflector traffic). Within the Razor system, edge systems (typically end users) collect hash values for messages received and are forwarded to central repositories which can then also be queried for matches against known UCE messages.

Given that cryptographic hash algorithms must produce differing results for messages that are distinct even in a single bit, circumvention of a naïve implementation is trivial by simply inserting small random variations into the UCE messages. To avoid this vulnerability, Razor uses a fuzzy signature matching algorithm based on a statistical model for messages [12], which is assumed to fulfill the following criteria:

- The digest identifying each message should not vary significantly for changes that can be produced automatically.
- The encoding must be robust against intentional attacks.
- The hash encoding should provide low risk of false positives.

As may be expected, however, there is a risk for the generation of false positives both owing to legitimate message traffic patterns and limitations of the fuzzy hash algorithm used. To remedy this problem, Razor requires feedback from users on which messages to classify as spam and which to whitelist.

C.6 Distributed Checksum Clearinghouse

The Distributed Checksum Clearinghouse (DCC) is based on the same general principles of fuzzy distributed hashing as Razor (see section II-C.5) and in fact uses the same hashing algorithm [12], [13].

However, unlike Razor it does not depend on user feedback. Every MTA or MUA that is DCC-enabled forwards messages it receives to DCC servers. The DCC servers then determine the number of similar messages and returns this count to the reporting system. A threshold value can then be used to classify a message as bulk or spam email.

In addition to the problems identified in section II-C.5, the DCC approach cannot identify legitimate bulk messages such as mail reflector or other solicited newsletter traffic and must therefore be combined with white-listing techniques or other approaches to avoid excessive false positive rates.

D. Content-Based Antispam Mechanisms

As a control, a content-based mechanism was also included in the experiment; the control selected for use in direct comparison was the widely used Spam Assassin package.

D.1 Spam Assassin

Spam Assassin considers both header and message body data in its calculations to determine the probability that a given message is to be considered UCE [14]. To this end, it applies a large set of rules, typically consisting of regular expression filters, to header and body material, and assigns a score to each rule (e.g. a message body containing a stock alert would add 2.362 points to the total sum while a message also containing the word “free” in the `From` address would add 0.194 points). The sum over all matching rules results in the total score or confidence value; if this exceeds a threhold, the message can be rewritten either by adding a header containing the score or by encapsulating the message in another MIME wrapper.

While Spam Assassin also supports DNS and checksum filters, these were not activated in the course of the experiment as these would replicate the behavior of systems described in sections II-C.4, II-C.5, and II-C.6, respectively. Moreover, Spam Assassin also supports Bayesian filtering, which provides a machine learning mechanism for classifying messages as UCE. Since this also requires continuous feedback and the use of training data sets, this feature was also not used for the purposes of the experiment.

III. Results

The effectiveness of the mechanisms used when viewed individually differs significantly. Figure 1 shows the false positive classifications when measured against the baseline data only, while figure 2 identifies the corresponding false negative classifications for each individual classification mechanism (note the different scales for each of these cases).

Both figures 1 and 2 were obtained by using the previously described metrics over the baseline data set; the validity of these measurements can best be compared to the oracle data obtained for the baseline data set; figure 3 provides an overview of the deviations in the detected and predicted classification results.

Figure 4 provides a direct comparison of content-based filtering using the SpamAssassin system at varying thresholds (see section II-D.1) with a combination of the blacklisting approaches, the greylisting, and the Razor distributed checksum mechanism. As can be seen in figure 4 when compared to the expected proportion of UCE messages, a threshold between 5 and 8 for SpamAssassin is the maximum sensitivity desirable before the selectivity of this approach suffers. For comparison, figure 5 illustrates the

1-4244-0130-5/06/$20.00 ©2006 IEEE

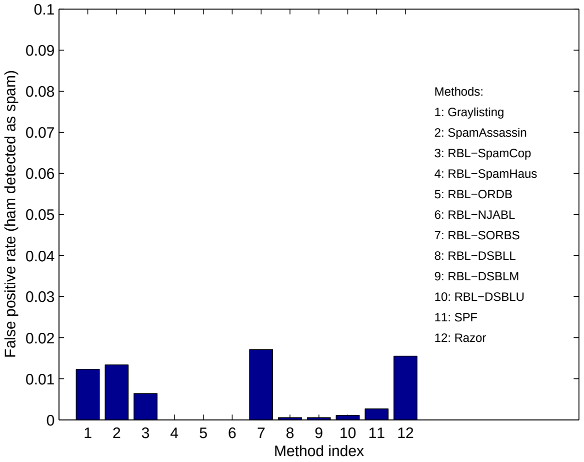

Fig. 1. Comparing false positive spam detection rates

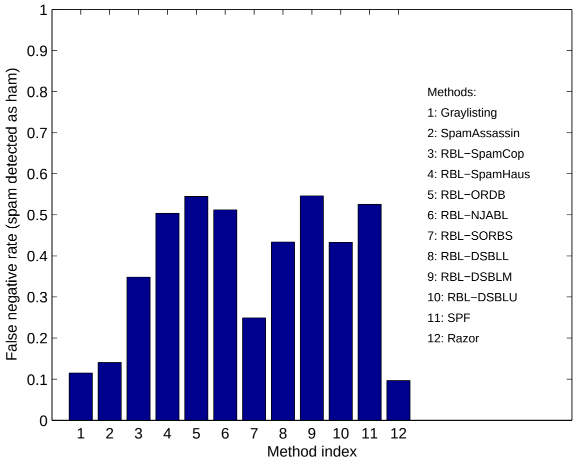

Fig. 2. Comparing false negative spam detection rates

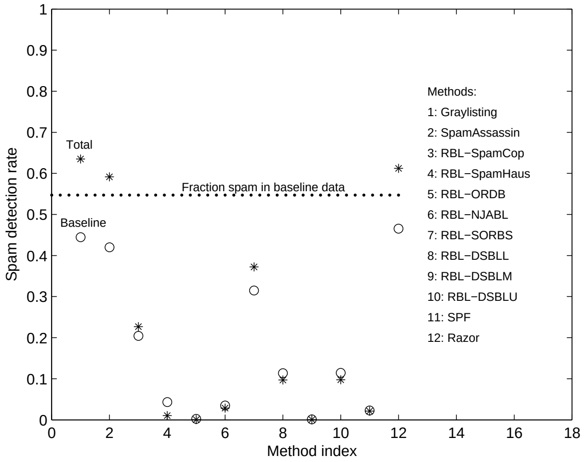

Fig. 3. Baseline and long-term measured UCE probabilities

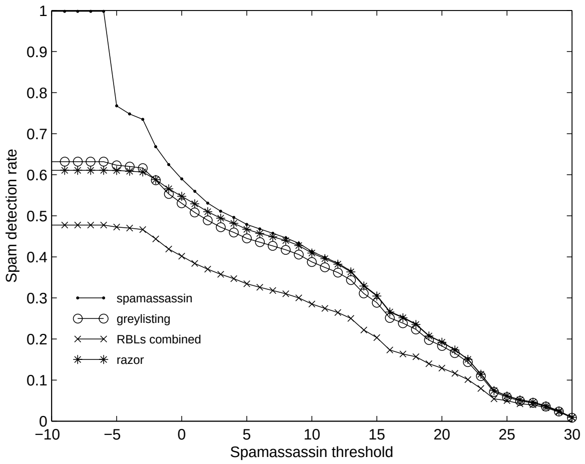

Fig. 4. Comparing classifiers with SpamAssassin thresholds

intrinsic tradeoffs encountered with setting thresholds on the experimental data set.

Finally, figure 6 provides a visual comparison of the receiver operating characteristics of the SpamAssassin classification mechanisms when varying the decision point [15], [16].

IV. Discussion

While the proportion of UCE messages reported in figure 3 is significantly lower than what has been reported earlier (see section V), it still constitutes more than half of the total message load handled by the electronic mail system.

The black-listing (RBL) mechanism is highly sensitive to the quality of maintenance and the aggressiveness of adding entries to the respective black lists, resulting in a more than 300% difference in both detection and also in the false-positive regimen.

The low detection rates shown for the SPF mechanism in figure 3 can, at the time of writing, be mainly attributed to the limited deployment of SPF. Given that SPF requires cooperation among sending entities and cannot make unilateral decisions, this approach may not become more prominent owing to a vicious circle of limited attractiveness to MTA operators while acceptance by MTA operators is still low.

The attractiveness of distributed checksum mechanisms, which show an attractive proportion of UCE messages classified positively, is somewhat hampered by the relatively high false-positive rate, which is particularly problematic for a multi-stage UCE filtering mechanism.

While greylisting proves to be highly attractive in terms of the classification results obtained, the use of greylisting

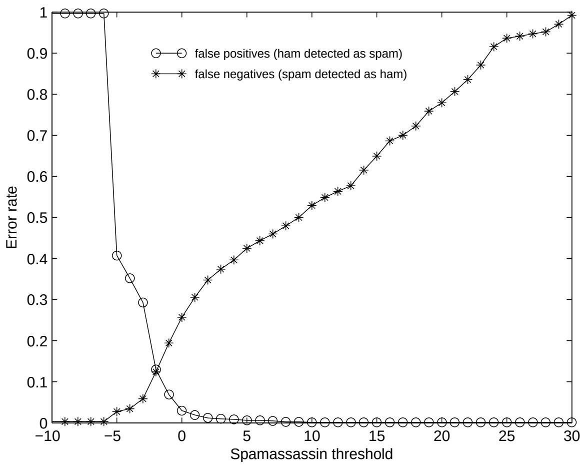

Fig. 5. SpamAssassin classification threshold characteristics

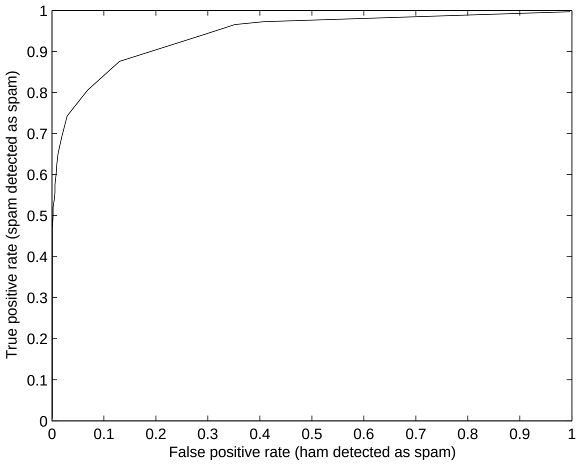

Fig. 6. Receiver Operating Characteristic (ROC) curves for the SpamAssassin classification mechanism

is at least somewhat controversial. The primary reason for this is the additional load on the sending MTA systems required for multiple communication attempts in case no previous listing exists. Even though (as discussed in section II-C.1) individual communication graphs appear to follow a power-law distribution resulting in a relatively small total burden for first attempts at communication between parties, the imposition of additional messaging requirements is undesirable. Moreover, given greylisting's requirement for compliance to SMTP standard on the part of all sending MTAs, this behavior may exclude certain systems (e.g. MTAs with only intermittent connectivity) from communication or at least impose significant delays owing to further communication delays.

V. Related Work

The relative effectiveness of using simple black listing over time was investigated by Jung and Sit [17], who also compared longer-term developments while Schryen provides a formal model for spam delivery and defensive options [18].

Any new approach or combination of techniques must be measured against both the regular (legitimate) patterns for email traffic and the techniques applied by senders of UCE. Particularly the latter can change rapidly in response to countermeasures and must therefore be taken into account dynamically in the development and analysis of antispam techniques. Key metrics in this assesment and development process are factors such as the mail arrival process, email sizes, number of recipients per email, popularity, and temporal locality among recipients [19]. Siponen and Stucke provide a quantitative assessment of email traffic and UCE proportion for inbound messages in a large number of corporations [20].

A selection of individual detection techniques (RBLs, phrase matching, SA heuristics, and statistical metrics) was investigated within the context of a larger Internet service provider by Sergeant [21], analyzing both the sensitivity and selectivity of these techniques while Balvanz *et al.* conducted a somewhat informal evaluation which also included end-user oriented systems [22]. A detailed evaluation of cost aspects for statistical approaches was conducted by Gómez Hidalgo [23] while Zhang *et al.* conducted an analysis of statistical mechanisms including naive bayes, maximum entropy model, memory based learning, support vector machine and boosted approaches both for English and Chinese corpora [24].

VI. Conclusion

Efficient antispam techniques continue to play a vital role in ensuring the continued viability of one of the most important forms of electronic communication and must be continuously monitored for effectiveness to permit timely responses to new tactics by UCE originators. While elaborate content-based filtering mechanisms provide excellent classification results, such filters also consume considerable resources and can therefore not be used indiscriminately for cost and capacity reasons.

The antispam methods analyzed in this paper provide a useful first filtering step when either used individually or in some cases also in combination with one another and thereby reduce the workload imposed on a content-based filtering mechanism. The principal mechanisms analyzed in the experiment detected between 37% and 75% of putative UCE as predicted by the baseline analysis when applied individually. These mechanisms also provided a very low false positive rate, particularly when compared to machine learning approaches; given that in some jurisdictions the suppression of legitimate message traffic can be a criminal offense, this provides assurance that these techniques can be used without undue risk of rejecting legitimate messages.

Given the relatively low individual probability rates, it is desirable to combine several of the mechanisms discussed in this paper in a first stage. Depending on the acceptable network and computational load, such a combination could include greylisting, hash databases such as Razor, and realtime blacklisting. A second stage should then incorporate content-based mechanisms such as machine learning and feedback mechanisms to further enhance selectivity and sensitivity.

At the time of measurement, an effective and efficient combination of such pre-filters is constituted by the use of both greylisting and a combination of several black-listing services. It should be noted, however, that the relative efficiency of the RBL services is dependent on the constant maintenance and quality of data used in maintaining the RBL databases and may therefore change significantly over time. These mechanisms provide an adequate balance in their receiver operating characteristic and can therefore reduce the load on a secondary spam filtering mechanism significantly.

As has been demonstrated before [17], the analysis reported in this paper can only identify approaches that are effective for a limited duration in time as both UCE senders change tactics and the relative effectiveness of approaches change, e.g. by revisions to distributed checksum databases or maintenance issues with real-time blacklists. Over the period reported here (2005 through early 2006), these results were quite stable; however, it is neverthelesss important to reiterate these experiments and also to include newer and emerging approaches; the latter is of particular importance since the effectiveness of the SPF framework could not be conclusively established given the rather low number of sites operating this scheme.

Future research will be directed to providing quantitative metrics for the relative efficiency (particularly computational and memory efficiency) of these approaches; this can provide the basis for deciding on a multi-tier antispam architecture in cases where the distinction between the various approaches is less clear than given the present data.

References

[1] P. J. Denning, "Electronic Junk," *Communications of the ACM*, vol. 25, pp. 163–165, Mar. 1982.

[2] L. F. Cranor and B. A. LaMacchia, "Spam!," *Communications of the ACM*, vol. 41, pp. 74–83, Aug. 1998.

[3] E. Harris, "The Next Step in the Spam Control War: Greylisting." White paper, available at `http://projects.puremagic.com/greylisting/whitepaper.html`, Aug. 2003. Last accessed on February 22nd, 2006.

[4] H. Ebel, L.-I. Mielsch, and S. Bornholdt, "Scale-free topology of e-mail networks," *Physical Review E*, vol. 66, Sept. 2002.

[5] L. H. Gomes, R. B. Almeida, L. M. A. Bettencourt, V. Almeida, and J. M. Almeida, "Comparative Graph Theoretical Characterization of Networks of Spam and Legitimate Email." arXiv ePrint physics/0504025, Apr. 2005.

[6] M. W. Wong, "Sender Authentication: What To Do." White paper, available at `http://www.openspf.org/whitepaper.pdf`, July 2005. Last accessed on February 22nd, 2006.

[7] E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, and M. Thomas, "DomainKeys Identified Mail Signatures (DKIM)." IETF DKIM Working Group Internet-Draft, Feb. 2006.

[8] J. Posluns, ed., *Inside the Spam Cartel*. Rockland, MA, USA: Syngress Publishing, 2004.

[9] V. V. Prakash, "Vipul's Razor." On-line documentation set, available at `http://razor.sourceforge.net`, July 2005. Last accessed on February 22nd, 2006.

[10] V. V. Prakash and A. O'Donnell, "Fighting Spam with Reputation Systems," *ACM Queue*, vol. 3, pp. 36–41, Nov. 2005.

[11] P. Deepak and S. Parameswaran, "Spam Filtering using Spam Mail Communities," in *Proceedings of the 2005 Symposium on Applications and the Internet (SAINT'05)*, (Trento, Italy), pp. 377–383, IEEE Press, Jan. 2005.

[12] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati, "An Open Digest-based Technique for Spam Detection," in *Proceedings of the 2004 International Workshop on Security in Parallel and Distributed Systems*, (San Francisco, CA, USA), Sept. 2004.

[13] Rhyolite Software, "Distributed Checksum Clearinghouse." Online documentation set, available at `http://www.rhyolite.com/anti-spam/dcc/`, 2006. Last accessed on February 22nd, 2006.

[14] A. McDonald, *SpamAssassin: A Practical Guide to Integration and Configuration*. Birmingham, UK: Packt Publishing, 2004.

[15] F. Hsieh and B. W. Turnbull, "Nonparametric and Semiparametric Estimation of the Receiver Operating Characteristic Curve," *Annals of Statistics*, vol. 24, pp. 25–40, Jan. 1996.

[16] V. Bewick, L. Cheek, and J. Ball, "Receiver Operating Characteristic Curves," *Critical Care*, vol. 8, pp. 508–512, Nov. 2004.

[17] J. Jung and E. Sit, "An Empirical Study of Spam Traffic and the Use of DNS Black Lists," in *Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement*, (Taormina, Sicily, Italy), pp. 370–375, ACM Press, Oct. 2004.

[18] G. Schryen, "A Formal Approach towards Assessing the Effectiveness of Anti-Spam Procedures," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, vol. 6, (Kauai, HI, USA), IEEE Press, Jan. 2006.

[19] L. H. Gomes, C. Cazita, J. M. Almeida, V. Almeida, and W. Meira, Jr., "Characterizing a Spam Traffic," in *Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement*, (Taormina, Sicily, Italy), pp. 356–369, ACM Press, Oct. 2004.

[20] M. Siponen and C. Stucke, "Effective Anti-Spam Strategies in Companies: An International Study," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, vol. 6, (Kauai, HI, USA), IEEE Press, Jan. 2006.

[21] M. Sergeant, "Internet Level Spam Detection and SpamAssassin 2.50," in *Proceedings of the 2003 Spam Conference*, (Cambridge, MA, USA), Jan. 2003.

[22] J. Balvanz, D. Paulsen, and J. Struss, "Spam Software Evaluation, Training, and Support: Fighting Back to Reclaim the Email Inbox," in *Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services*, (Baltimore, MD, USA), pp. 385–387, ACM Press, Oct. 2004.

[23] J. M. Gómez Hidalgo, "Evaluating Cost-Sensitive Unsolicited Bulk Email Categorization," in *Proceedings of the 2002 ACM Symposium on Applied Computing*, (Madrid, Spain), pp. 615–620, ACM Press, Mar. 2002.

[24] L. Zhang, J. Zhu, and T. Yao, "An Evaluation of Statistical Spam Filtering Techniques," *ACM Transactions on Asian Language Information Processing*, vol. 3, pp. 243–269, Dec. 2004.