Comparative analysis of Anti-Spam Software Vendors

July 8, 2004

Bitspan Network Inc.
405-100 Park Royal South
West Vancouver, British Columbia
V7T 1A2
Canada

http://www.bitspan.net
Tel. 604.926.3242
Fax. 805.980.5348

Objective:

- To assess and compare the accuracy of spam detection technologies commonly deployed in popular email filtering applications against Bitspan FEST Agent 1.0
- To assess the value of integrating Bitspan FESTAgent 1.0 into existing anti-spam filtering applications to reduce false negatives[1] and false positives[2].

Methodology:

- To achieve the objectives set forth in this controlled study, we focused our testing on obtaining false negative and false positive rates as well as actual catch rates of various popular client-side mail filtering application.
- In this study, we selected 4 products: Microsoft Outlook 2003 with its native mail filtering technology, McAfee's SpamKiller 5.0, Symantec's Norton Antispam 2004, and Bitspan FEST Agent 1.0 for Microsoft Outlook. The products were installed on separate but equivalent systems and the latest software updates were applied. Although, each product offered varied levels of protection, no changes were made to the settings -- the default settings were selected.
- The email client for all was Microsoft Outlook XP with the exception of Microsoft Outlook 2003. The email clients were configured to receive the same emails near simultaneously. The process ran for a period of 72 hours. During this period each account received 11459 of which 8410 emails were legitimate and 3049 were spam -- Text and HTML formats. Performance was not measured, however it seemed reasonably acceptable.

Results:

Application	Catch Rate (%)	False Negative (%)	False Positive (%)	False Negative Correction (%)	True Spam Verification (%)
Microsoft Outlook 2003	31	69	0.7	34	47
Norton AntiSpam 2004	50	50	4	45	53
McAfee SpamKiller 5.0	56	44	57	38	54
Bitspan FEST Agent 1.0	**47**	**53**	**0**	**Not Applicable**	**Not Applicable**

[1] False negative is the incorrect identification of spam email as legitimate.
[2] False positive is the incorrect identification of legitimate email as spam.

Catch Rate comparison

In the first test, we compared catch rates of the selected applications. The catch rate reflects the percentage of spam emails that were correctly identified as spam by the application. This figure does not include false negative and false positive rates.

Application	Catch Rate (%)	False Negative (%)	False Positive (%)	False Negative Correction (%)	True Spam Verification (%)
Microsoft Outlook 2003	**31**	69	0.7	34	47
Norton AntiSpam 2004	**50**	50	4	45	53
McAfee SpamKiller 5.0	**56**	44	57	38	54
Bitspan FEST Agent 1.0	**47**	53	0	Not Applicable	Not Applicable

As table (above) clearly shows, McAfee's SpamKiller 5.0 had the highest accuracy catch rate at 56% and Microsoft's Outlook 2003 had the lowest at 31%. Although an application's catch rate is a valid number to consider when selecting a mail filtering technology, by itself it is not a good measure of assessing an application's filtering abilities over another. Other factors such as false negative and false positive rates also need to be considered.

False Negative rate comparison

In the second test of this study, we measured the false negative rates of each the selected applications. These were percentage of emails that were clearly spam but were not filtered out and remained undetected in the "Inbox" of Microsoft Outlook. The results are shown in the table below.

Application	Catch Rate (%)	False Negative (%)	False Positive (%)	False Negative Correction (%)	True Spam Verification (%)
Microsoft Outlook 2003	31	**69**	0.7	34	47
Norton AntiSpam 2004	50	**50**	4	45	53
McAfee SpamKiller 5.0	56	**44**	57	38	54
Bitspan FEST Agent 1.0	47	**53**	0	Not Applicable	Not Applicable

In our study, Microsoft's Outlook 2003 recorded the highest false negative rate at 69% while McAfee's SpamKiller 5.0 had the lowest false negative rate at 44%. Although false negative rate is important gauge by itself, it is not a good measure of efficacy of an email filtering solution and other parameters such as false positive rate must also be considered.

False Positive rate comparison

In part 3 of this study, we measured the respective false positive rates of the selected applications. False positives reflect errors in algorithm that result in inaccurate identification of legitimate emails as spam. In most cases, this problem remains hidden from end-users since such emails are either deleted or commonly quarantined for a finite period of time and are not readily accessible. In the case of the later, locating such emails is difficult and expensive since searching for legitimate emails in a large pool of spam emails is like looking for a needle in a hay stack. This remains the biggest weakness of many of today's mail filtering technologies and is the focus of research by many. A technology is desirable if it proves to have the lowest count, if not zero, of false positives.

Application	Catch Rate (%)	False Negative (%)	False Positive (%)	False Negative Correction (%)	True Spam Verification (%)
Microsoft Outlook 2003	31	69	**0.7**	34	47
Norton AntiSpam 2004	50	50	**4**	45	53
McAfee SpamKiller 5.0	56	44	**57**	38	54
Bitspan FEST Agent 1.0	47	53	**0**	Not Applicable	Not Applicable

As depicted in table (see above), Bitspan FEST Agent 1.0 scored the lowest false positive rate of all. Bitspan FEST Agent 1.0 scored a solid 0 percent meaning it did not make any errors in identification of emails. Bitspan FEST Agent 1.0 was followed by Microsoft Outlook 2003, Symantec's Norton Antispam 2004 and McAfee's SpamKiller 5.0.

False Negative Correlation rate

In part 4 of the study, we proceeded to determine how Bitspan FEST can complement existing mail filtering technologies. This test can only be conducted when Bitspan FEST Agent is implemented in conjunction with another mail filtering application or technology.

We measured Bitspan FEST Agent's ability to reduce false negative rate of an existing mail filtering application. To do this we scanned the undetected spam emails (the false negatives from test 2) using Bitspan FEST Agent 1.0. The theory is that any email caught by Bitspan FEST Agent 1.0 would be additional spam email that could be caught if the Bitspan FEST is embedded within each of the tested applications. The results are depicted in the table below.

Application	Catch Rate (%)	False Negative (%)	False Positive (%)	False Negative Correction (%)	True Spam Verification (%)
Microsoft Outlook 2003	31	69	0.7	**34**	47
Norton AntiSpam 2004	50	50	4	**45**	53
McAfee SpamKiller 5.0	56	44	57	**38**	54
Bitspan FEST Agent 1.0	47	53	0	**Not Applicable**	Not Applicable

The average false negative correction rate was 39%. This means that the overall false negative rate can be reduced (on average) by as much as 17% for each of the tested applications if Bitspan FEST Agent 1.0 is also used is filtering emails. This would mean less number of emails would end up in a user's mailbox, which should help enhance mail service experience for end-users as well as help reduce storage and network traffic for an organization that support such users.

True Spam Verification

In part 5 of this study, we measured the spam verification abilities of Bitspan FEST Agent against previously identified spam. This test can only be conducted when Bitspan FEST Agent is implemented in conjunction with another mail filtering application or technology.

To perform this test, we scanned emails previously identified as spam (by another email filtering application/technology) with Bitspan FEST Agent 1.0. The said emails had be isolated and quarantined by all of the applications in a separate Microsoft Outlook folder. The results are reflected in the table below.

Application	Catch Rate (%)	False Negative (%)	False Positive (%)	False Negative Correction (%)	True Spam Verification (%)
Microsoft Outlook 2003	31	69	0.7	34	**47**
Norton AntiSpam 2004	50	50	4	45	**53**
McAfee SpamKiller 5.0	56	44	57	38	**54**
Bitspan FEST Agent 1.0	47	53	0	Not Applicable	**Not Applicable**

On average Bitspan FEST Agent 1.0 was able to certify the spamity[3] of 51% of isolated spam emails. This means that theoretically, it is possible to conclude that since 2 different technologies (one of which has a zero false positive detection rate) have concluded that an email is spam, therefore, about 51% of quarantined emails can be discarded permanently and with confidence thus reducing storage and network traffic and also help enhance the overall end-user experience with the solution.

In addition, a value that this process brings to the picture is that, since the size of the junk or quarantine folder is 51% smaller, it is theoretically more feasible to detect false positives for an end-user. Furthermore, by identifying false positives, a mail system administrator or person in charge of mail filtering algorithm(s) can quickly identify errors and proceed to apply fixes that are aimed at reducing errors in the native application algorithms (client and/or server side). Hence, one can look at this collaboration of technologies as means to debug existing algorithms.

[3] Spamity® is an email's quality or state of being a spam. This quality or state is measurable via different means and henceforth it is this overall measure that determines whether an email is spam or not. Spamity® is a registered trademark of Bitspan Network Inc.

Conclusion

From these results, one can conclude that with the exception of Bitspan FEST Agent 1.0, all of the tested products resulted in false positives. No single application was able to correctly filter 100% of emails. Furthermore, tests showed that Bitspan FEST Agent 1.0 could complement existing filtering methodologies by reducing the false negative rates of all of the tested applications by an average of 39% and the overall catch rate by 17% without compromising the false positive rates. Lastly, we tested the ability of Bitspan FEST to re-verify or certify decisions made by other mail filtering applications. The results showed that, on average, Bitspan FEST was able to identify about 51% of previously isolated spam email. Given Bitspan FEST Agent's zero false positive rate, its implementation as the only filtration system, can provide a sound filtering solution that guarantees delivery of legitimate emails. Furthermore, its implementation in conjunction with existing native technologies could help reduce false negatives and false positives and hence help improve efficacy of mail filtration solutions.

Although this study focused on end-user (client-side) mail filtering systems, it is theoretically possible to conclude that similar results can be obtained if Bitspan FEST is implemented at such as SMTP, MTA[4], or other levels.

[4] MTA or Message Transfer Agent.
Unlike an MTC, the MTA actually handles sending and receiving the email to and from the system it is based upon. Most MTAs support aliasing and forwarding, as well as either the POP or IMAP protocols for clients which do not have standard MTA support upon their computer. MTAs which support POP and/or IMAP are referred to as mailhosts, and often support other functions. At UCI, MTAs are used to accept mail from the network and the outside world, then forward the mail to specific places. Mail address to user-id@uci.edu goes through campus MTAs for translation to delivery points, and actual delivery.

About Bitspan

Bitspan Network Inc, headquartered in West Vancouver, British Columbia, Canada specializes in developing state of the art anti-spam technology for use in existing message filtration systems.

Bitspan FEST Agent 1.0, is a registered product of Bitspan Network Inc.

For more information, please visit us at http://www.bitspan.net or contact us at 604-926-3242.