The Monthly GNU Column

BRAVE GNU WORLD

This column looks into projects and current affairs in the world of free software from the perspective of the GNU Project and the FSF. In this issue, we focus on Amavisd-New, a new daemon that operates as a spam filter. **BY GEORG C.F. GREVE**

The computer industry has not found an easy solution to the problem of spam. Solutions vary, but combination of various approaches seems to make the most sense.

One of the most useful approaches is to allow the mail server to filter messages before forwarding them to the user. Many projects are working on this problem, and we have looked at some of them in this column, SpamAssassin [5] for example. But this month we'll focus on a different approach: filter networks. Many administrators have started applying multiple filters, combining spam and antivirus scanners, for example, or using multiple filters to achieve more hits. There are no limits to the effort you can put into this, but the more complex a system becomes, the more susceptible it is to configuration errors.

Amavisd-New

The Amavisd-New [6] project is an attempt to develop an interface between the Mail Transport Agent (MTA) and various scanners or filters. The name actually derives from the Amavis (A Mail Virus Scanner) [7] project. Many system administrators have been using this software for years.

The Amavisd-New program was developed on the basis of the original daemon component back in 2002. Within the scope of his activities at the Jozef Stefan Institute [8] in Ljubljana, Slovenia, developer Mark Martinec suggested so many changes to Amavis that it would have been impossible to add them to the original code base.

This led to a split in development activities, and after three years of hard work, the Amavisd-New project has hardly anything in common with its ancestor. Amavisd-New has a lot more code, better performance, more features, and a more exact implementation of various standards. Despite this, the program is still compatible with external modules for the original Amavisd. A virus-only scanner has thus made a transition to a high throughput and extremely reliable interface between the MTA and one or more message scanning programs.

Amavisd-New runs as a server daemon with extremely sophisticated process management. Using a similar approach to the Apache web server, the daemon launches a number of process to anticipate requests, thus reducing the handling time. Users can communicate with the software via an RFC 2033-compliant LMTP server, an RFC 2821-compliant SMTP server, and an SMTP client. Amavisd-New generates RFC 3462 and RFC 3464-compliant status delivery messages and supports external program modules.

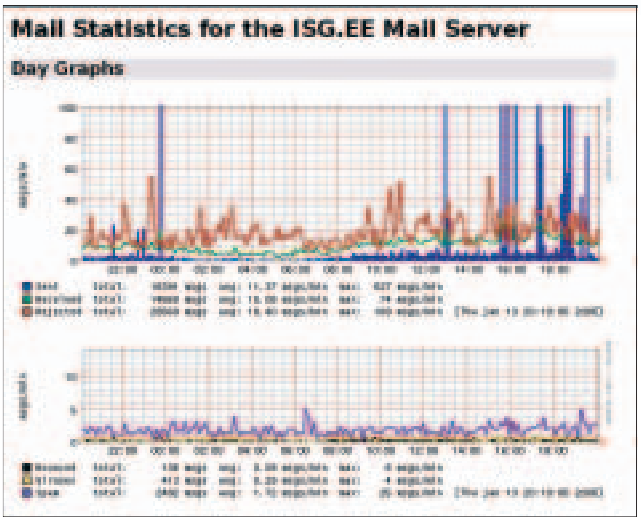

Figure 1: The Mailgraph program gives administrators a useful graphical display for mail traffic analysis.

Details

Amavisd-New was written in Perl, and this makes it highly platform independent, easy to maintain, and reliable. In particular, using the Perl scripting language removes the danger of buffer overflows or invalid pointers, and thus prevents two popular attack vectors designed to take down the scanner or break into the system. Mark emphasizes the security aspect as one of the program's major strengths. Conscientious bug hunting, informative error messages, and failsafe mechanisms all help to underline this claim. And if this is not enough for you, you can run the program in a chroot jail to further mitigate the effect of a potential compromise.

Figure 2: Even though the idea of a sender ID may seem to make sense at first, it is fraught with danger due to the Microsoft patents on the method.

Mark points to more advantages: the program supports a variety of (non-free and free) anti-virus scanners, and Amavisd-New is free software itself released under the General Public License (GPL). The program has advanced optimization features, which can be fine tuned by reference to an internal performance and statistics database. Third-party tools, such as Mailgraph [9] by David Schweikert, which gives administrators useful statistics on received, sent, or rejected messages (Figure 1), can also facilitate the optimization process.

Future Plans

Although Mark Martinec recommends Postfix [10] as an MTA in combination with Amavisd-New, the program will work with other MTAs, although this may mean losing some functionality. The project is extremely popular within the Postfix community, and it has provided years of useful service at some locations.

In the future, Mark is planning to make the development process more professional, using bug tracking, public source code management, and better documentation to give more developers the opportunity to join in with the development process.

New Tricks

Spammers are constantly devising new ways of tricking or undermining filters; and future development will need to react to these attempts. However, the next item on the roadmap is a secure and reliable method of unpacking CPIO and tar archives. If you are interested in getting involved with the Amavisd-New project, check out the Amavis-User mailing list – you'll find a long list of things to do at [11].

Last Words

When all is said and done, beating the spam issue will mean users needing to change their habits. One basic rule for beating spam might be to stop sending mail messages with HTML content. HTML messages are unnecessary and downright dangerous, as the MIME standard supports embedding of multimedia content. Inexperienced users in particular tend to use HTML messages, as they are often unaware of the fact that the link label need not have anything to do with the target for that link.

There is another basic rule for handling spam: delete immediately. Answers just indicate to the spammer that the account is alive. ■

Best Laid Plans

Even the best laid plans can fail due to faulty implementation. In the case of mail filters, this happens if the filter is badly configured. Tagging MIME-compliant or digitally signed email messages as spam is a typical example of this.

Besides the thousands of good ideas that become bad ones due to faulty configurations, there are thousands of really bad ideas. And bad ideas that look good at first glance are always the worst.

Approaches such as Microsoft's sender ID (Figure 2) are at the top of the list of bad ideas. The software giant argues that spammers misuse anonymity to do mischief. And this is why MS thinks that it is a good idea to be able to track email messages back to their source. But as the Apache Foundation and other organizations point out, the fact that Microsoft has patented this mechanism would give the monopolist perfect control of email as a medium.

Apart from this, the sender ID does not come up with the goods. For one thing, identities can easily be forged; for another, spoofing IDs is one of the classical crimes in this age of information technology. Compromised machines often give attackers a platform from which they can distribute spam – and a sender ID will do nothing to change this.

Now that AOL has protested against the idea, one can only hope that MS will shelve its plans. But there is no way of knowing when the ghost might come back to haunt us.

INFO

[1] Send ideas, comments, and questions to Brave GNU World: *column@brave-gnu-world.org*

[2] GNU project homepage: *http://www.gnu.org/*

[3] Georg's Brave GNU World homepage: *http://brave-gnu-world.org*

[4] "We run GNU" Initiative: *http://www.gnu.org/brave-gnu-world/rungnu/rungnu.en.html*

[5] SpamAssassin homepage: *http://spamassassin.apache.org*

[6] Amavisd-New homepage: *http://www.ijs.si/software/amavisd/*

[7] Amavis homepage: *http://www.amavis.org*

[8] Jozef Stefan Institute homepage: *http://www.ijs.si*

[9] Mailgraph homepage: *http://people.ee.ethz.ch/~dws/software/mailgraph/*

[10] Postfix homepage: *http://www.postfix.org*

[11] To-do list for Amavisd-New: *http://www.ijs.si/software/amavisd/TODO*