SECURING THE EMAIL SERVICES
New System for Secure Managing the Organization's Mail Service

Raúl Herbosa
Computer Systems Director, Grupo Tecnológico e Industrial GMV S.A., C/Isaac Newton, 11
Parque Tecnológico de Madrid, 28760 Madrid, Spain

Gabriel Díaz and Manuel Castro
Electrical and Computing Engineering Department, UNED (Spanish University for Distance Eeducation)
c/Juan del Rosal, 12 – Ciudad Universitaria, 28040 Madrid, Spain

Keywords: Spam, email, virus, phishing, malware, GPL, open source, secure management, email services.

Abstract: In this paper new system is presented for securing the email service, minimizing the risks associated with spam and malicious software associated with the email messages, valid for any organization. To build it, several free software tools under GPL license are used, integrated over a generic hardware platform. The approach has been the typical of an integration project. The concrete needs have been identified, related to email threats, free software tools under GPL have been identified that meet our needs and the integration tasks have been made, suggesting hardware and software architecture to support our objectives. One crucial criterion for the selection has been that the tools must provide working information records, i.e. file logs and tools to treat them for the different covered subsystems. Several tools have been developed also to complete the original functionality of them. The resulting system, nowadays in use in a big company in Spain, is a flexible and effective one, that filters quickly and exhaustively every incoming and outgoing message, eliminating successfully more than 80% of the received messages, that result to be spam or malware.

1 INTRODUCTION

We live in a world in which it's difficult to discuss the outstanding importance of the electronic mail for the business and the normal and usual way of doing anything for any organization, from the small ones to the big ones. However, we face a growing quantity of threats to the correct functioning of this critical service.

The attacks to this service have different objectives: from denial of service attacks (mail bombings) for avoiding the use of the service to the ubiquitous spam, attacks through mails containing virus and different kind of malware, etc.

Only speaking of spam, a MessageLab report (MessageLabs, 2008) estimates that, in January 2008, more than 73 percent of email was spam. Also you can find very different approaches (Kim et al, 2007) trying to repair the problem.

It is also remarkable, for example, to see how anyone can get very rich and resourceful information on how to spam in Internet (Graham, 2007), in which you can obtain very easy and detailed information on the plan to spam, step by step in a variety of forms.

On the other hand, taking into account that the perimeter firewalls can not block the SMTP mail traffic, because this situation would stop the legitimate mail, the mail server has become the ideal target for the sending of virus and malware, like spyware, hoaxes, phishing, etc., that must be taken into account when you design the solution for a secure email service.

2 CURRENT APPROACHES TO A SOLUTION

It is possible to find nowadays different solutions, commercial ones and also based on open source software (Goodman et al, 2007) that, by different techniques, suggest different improvements for the problem's solution. We can classify them in two

Herbosa R., Díaz G. and Castro M. (2008).
SECURING THE EMAIL SERVICES - New System for Secure Managing the Organization's Mail Service.
In *Proceedings of the International Conference on Security and Cryptography*, pages 469-472
DOI: 10.5220/0001915804690472

main groups: preventive strategies and corrective strategies.

In the side of the preventive strategies we can find several efforts for minimizing the threats and, as consequence, the risks associated to be attacked. One of them is to establish a corporative policy for the use of email, another to protect the email address, by not publishing it in non secure webs, or by using obfuscators.

Some of the corrective strategies try to avoid that, once the attack initiated, the spam or infected mail, arrive its target, but allowing the valid messages. We can find also two broad classes, one is a technique based on the message content and the other not based in the content.

The techniques based in the message content analyze this and the subject header in search of a set of words that reflect the kind of message, using basic filters, , heuristic filters, or bayesian filters (Li et al, 2006), that learn to distinguish the valid (ham) mails and the spam.

The other techniques are based in other different characteristics in the message content, as the name of the source server or its IP address:

- Black lists, IP addresses lists that must be blocked because they are known as spam sources.
- White lists, lists with trusted sender IP addresses.
- Distributed filters (DCC, Distributed Checksum Clearinghouse). In this case the user marks any message he considers to be spam, then DCC program generates a signature identifying the message and sends it to the DCC servers, that are updated daily, as the pay service referenced in www.cloudmark.com.
- Grey Lists or challenge/response.
- Sender Policy Framework, an emerging standard in which the domain owners designate their email servers in DNS in a predefined way (using SPF registers) that let the email messages receivers to check if it is a legitimate message sent by the email server associated to the domain specified in the sender.

But what it is not possible to find, at least in the open source arena, is a complete and easy to manage and effective system, and we thought a good idea was to develop an exhaustive control of the problem in a continuous, adaptive way, really a securely managed service.

To face the problem we began studying a new possible protection architecture.

3 PROTECTION ARCHITECTURE FOR THE EMAIL SERVICE

If it is assumed that it seems impossible to stop the attacks and malware infections with a 100% of success, and that the attackers are more dynamic than the developers and builders of protection products, it is crucial to understand that it must be the infrastructure itself the responsible of the constant and continuous protection against the possible (very probable) unwanted effects.

It must be provided a multilevel architecture that channels and minimizes the impact of a protection level with respect to the next one, and such that the possible vulnerabilities of a level doesn't affect the following one. In this way we can consider each level an independent sub-service, which must be protected.

One of the main pillars in this architecture is that the mailboxes are not in the same server that receives the messages from Internet. This allows an easier protection of the stored user content, not being affected in the case of having being attacked successfully one of the front levels.

Other important consideration is to oblige any message sent from within our organization to go through the same levels that a received message. The objective is to minimize the risk window associated with the corporative electronic mails.

Taking all that into consideration we can define the different protection levels, illustrated in Figure 1.

3.1 Multilevel Architecture

We can differentiate 5 different levels in the architecture:

1- Front-end shell: The first line of defence, exposed directly to Internet. We place here the email server published in the DNS server for our organization domain, the server target of any world wide email server for sending email messages to our organization.

2- Corporate firewall: We can include a strict filter in our firewall defining our front-end email server as the only machine that can introduce email messages in our internal network. On the other hand, nobody from the internal corporate network can send email outside without using the front-end email server (the firewall is instructed to).

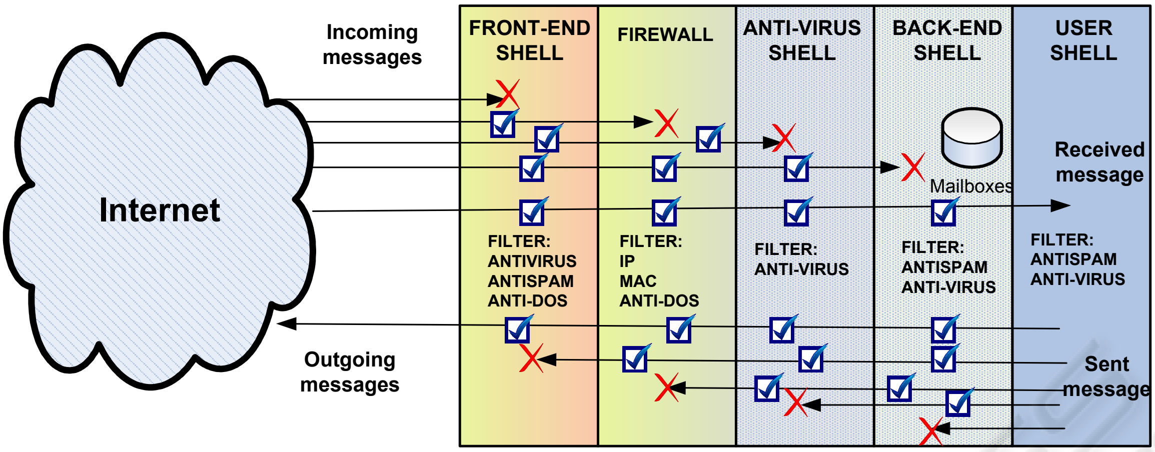

Figure 1: Security multilevel architecture for the e-mail services.

3- Corporative antivirus: We deliver here a mechanism for minimizing the risk window associated with antivirus protection.

4- Corporative back-end: This shell contains all the users’ mailboxes, so it must be very well protected from external attacks as from internal attacks.

5- User shell: In this shell we do the last anti-spam and antivirus control to the received messages as well as to the sent messages, generated by the user.

Also, for all the internal allowed communications between the different level machines, we use cryptographic protocols such as ssl, Kerberos, etc, not allowing the communications being in clear text through the internal network.

This multilevel architecture allows isolating the consequences of a concrete problem and identifying the grade of intrusion. We decided to implement a solution for the most critical shell from the point of view of security and protection, the most external one.

4 OUR COMPLETE SOLUTION FOR THE FRONT-END SHELL

Due to the asynchronous characteristics of the reception of mail and of the latency produced by Internet in the communication between servers, it is not necessary to have an special platform, so we use one of the typical PCs used by users in our organization. We manage a volume of more than 20000 messages by day without provoking any kind of additional latency in the correct reception, filtering an resending of the corporative messages.

We have integrated the set of tools detailed in Table 1, and some special considerations are:

- Sendmail can’t interact directly with SpamAssasin and ClamAV and so it must use the MILTER (Mail Filter) libraries.
- We provide some perl scripts and a web page to make related administrative tasks.

Table 1: Details of each used tool in the system.

Used tool	Version
Operating system	Fedora 7 x86_64 LINUX
MTA	Sendmail.x86-64 8.14.2
AntiSpam Filter	Spamassasin.x86-64 3.2.4
Antivirus	clamav.x86-64 0.92.1
Filtering framework	mimedefang.x86-64 2.64
O.S. securization tool	Bastille-3.0.9-1.0
Logs analyzer	Graphdefang-0.9
IDS tool	Psad-2.1.1

The complete proposed software structure is illustrated in figure 2. The sendmail program, in its normal work, uses two different processes: one of them listens in the port 25 and put every received message in a specific queue, say queue 1. After this, all the antispam and anti-DOS capabilities configured in sendmail are applied. The second process is permanently watching another queue, say queue 2, and when a message appears in this queue will be delivered to its destiny, local or remote.

The work done by MIMEDefang is precisely taking the messages from queue 1, and send them to the ClamAV and SpamAssassin processes to search for the presence of virus or spam respectively and, if it is determined that they are not malicious by the two processes, MIMEDefang process write a log line per message and send them to queue 2.

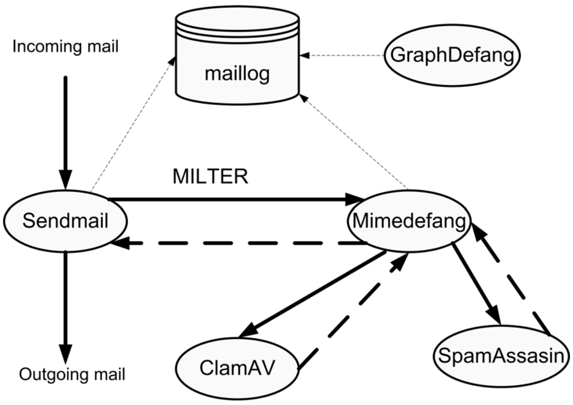

Figure 2: Structure proposed for the processes intervening in the securized email front-end

For the hardening of the operating system we use the BASTILLE program, configure the Linux IPtables firewall in the way that just the needed ports are open and use the PSAD (Port Scan Attack Detector) program, a typical IDS (intrusion detection system).

One of the most practical mechanisms we use to control our system is the statistics of use to identify the volume of information transmitted through our system and the system's efficacy. We represent by graphs statistical data related to efficacy of the filters and controls, time distribution of the attacks, identified attackers and so on.

We enter through a typical web page (Figure 3) where we see, first of all, two graphs with the total use of email messages for our organization and the Top 10 users.

If we decide to see in detail the "total" part of the data we can see the statistics in a hourly, daily or monthly period, always showing the ratio between rejected and accepted mails.

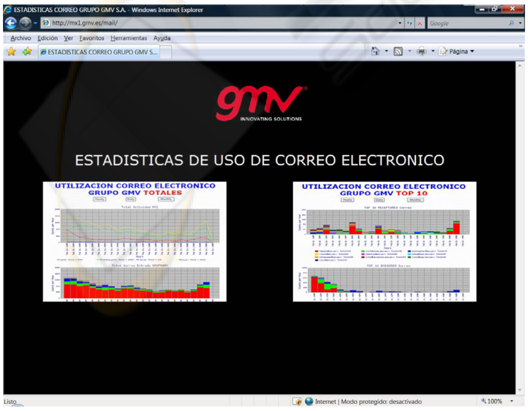
ESTADISTICAS CORREO GRUPO GMV S.A. - Windows Internet Explorer
http://mx1.gmv.es/mail/
Google
Archivo
Edición
Ver
Favoritos
Herramientas
Ayuda
ESTADISTICAS CORREO GRUPO GMV S...
Página
gmv
INNOVATING SOLUTIONS
ESTADISTICAS DE USO DE CORREO ELECTRONICO
UTILIZACION CORREO ELECTRONICO
GRUPO GMV TOTALES
UTILIZACION CORREO ELECTRONICO
GRUPO GMV TOP 10
Listo
Internet | Modo protegido: desactivado
100%

Figure 3: Home-page for the statistics of use for the e-mail services in GMV.

5 CONCLUSIONS

The proposed solution implements a complete protection system for the electronic mail service through the integration, configuration and development of 100% free components under GPL license. This system, now in production in a real company environment (GMV International Business Group, www.gmv.com), is obtaining very good results that exceed the effectiveness of most part of the commercial systems doing this function.

To develop the system we have followed an structured process, identifying each of the available software pieces in the GNU community with best performance and capacity and we have also configured and tuned them in a specific way to work together.

The system is successful in avoiding external attacks, sending alerts about the most persistent ones and about the most dangerous. The system eliminates more than 80% of the received messages that, if we didn't have this protection, should flood the users' mailboxes.

We follow trying to integrate new techniques and, why not, developing our own enhancements to the system.

ACKNOWLEDGEMENTS

The authors would like to acknowledge GMV International Business Group for their permission to publish private technical information and also to the Spanish Science and Education Ministry and the Spanish National Plan I+D+I 2004-2007 for the partial support in the project TSI2005-08225-C07-03 "mosaicLearning: Aprendizaje electrónico móvil, de código abierto, basado en estándares, seguro, contextual, personalizado y colaborativo"

REFERENCES

Goodman J., Cormack G.V., Heckerman D.,2007. *Spam and the ongoing battle for the inbox*, in Communications of the ACM, February 2007.

Graham, Paul, http://paulgraham.com/howspam.html.

Kim J., Chung K., Choi K, 2007. *Spam filtering with dynamically update URL statistics*, in IEEE Security & Privacy July/August 2007.

MessageLabs, 2008. *Spam: Business-Savvy Spammers Tout Bargain Mortgages and Search Engine Spam Revs Up*, intelligence report; http://www.messagelabs.com/mlireport/MLI_Report_January_2008.pdf.