This document is part of the project “Security in Communications: Quality Platform in the Electronic Mail Service” subscribed to the FRIDA program (Regional Fund for Digital Innovation in Latin America and the Caribbean). This project has articulated the creation of the HERMES platform (Towards an Environment of Secure Electronic Messaging). (http://hermes.runa.cl) constituted by different European and Latin American academic networks.

The following institutions from the academic networks took part in the creation of this document:

RETINA (Argentina) http://www.retina.ar
RNP (Brasil) http://www.rnp.br
REUNA (Chile) http://www.reuna.cl
RedIRIS (España) http://www.rediris.es

Code of best practices for the administration of the Electronic Mail Service in the Latin American Academic Community (RedCLARA).

Introduction

The electronic mail is a crucial and widely used application, especially within the collaborative environment of the academic world, and the problems affecting it are quite well known. The idea of this document is to establish a common framework to mitigate the security problems affecting electronic mail in the academic environment so that it can continue being a useful tool. A document of good practices intends to help all the actors involved to define and configure their Service with certain minimum criteria that certify the quality of the outbound and inbound SMTP traffic of their institutions.

The commitment to adopt these criteria is not only improving the service within the institution since it is generating a better quality NETWORK of services within the institutions adopting them. The adoption of these criteria by each of the institutions will result in a service of similar quality with a common basis, greater control and optimisation.

Additionally, the implementation of these recommendations will not only improve the quality of exchange of SMTP traffic. It will also help to reduce many of the security problems affecting the service: Spam, spoofing, malware, etc.

This document is mainly aimed at administrators of the electronic mail service of the Latin American academic world (universities, research centres, etc) but it could be applied in any other context.

To date, this code of good practices is being promoted in the institutions coordinated by the operations centres of the following academic networks:

RETINA (Argentina) http://www.retina.ar
RNP (Brasil) http://www.rnp.br
REUNA (Chile) http://www.reuna.cl
RedIRIS (España) http://www.rediris.es

It is expected that the list will grow and with the incorporation of the other Latin American academic networks it will be achieved the goal of improving the quality of the electronic mail service.

Model of Electronic Mail Service

This document of recommendations is adapted to a model of centralised electronic mail service. This model articulates all the Central *Office*[1] Service (Level 1) through which all incoming and outgoing mail will have to be directed. This office will be the engine of a hierarchic structure of servers (Level 2, Level 3, etc) that will completely configure the routing map of an Electronic Mail Service within the institution.
Under certain circumstances this model can be more flexible and implement some degree of direct routing allowing the existence of several Level 1 *Offices* that directly route to/from the Web. The team responsible for the Institutional Service must coordinate this alternative. What has to be avoided is the appearance of mail servers with direct routing in centers, departments, faculties, etc, belonging to the organization offering the service. This situation will result in an increase of **islands** that will impair the management and evolution of the Service.

Two mainly independent servers constitute a Main or Level 1 *Office*:

- **System of SMTP traffic routing**, mail relay. This machine is responsible for:
  1. Accepting SMTP external connections (Internet) to deliver them to the storage System.
  2. Accepting internal SMTP connections (ports 25 and/or 587) from our institutions to the exterior (Internet).
  3. Respond to the MX registers of the permitted domains.

- **System of users' mailbox storage**. This machine is responsible for:
  1. Accepting SMTP connections only from the routing System to store them in the mailboxes.
  2. Allow users to access their mailboxes.

It is very important to stress that both systems should be physically separated in order to isolate the mailbox system from possible attacks.

This centralized model concentrates the human and technical resources in a defined group of servers, which allows an optimum operation, high reliability and availability of the service. Additionally, it creates a single point of contact with users, facilitates the implementation of new technologies in the Service and makes it possible to set common policies for all the institution.

The recommendations in this document are directed at all the Level 1 mail servers of the Institution.

Structure of the Document:

[1] Office is a courier, MTA or mail relay.

The document is divided into two groups of Good Practices Criteria:

- **Basic Criteria**. They are described as those criteria that are essential for the minimum functioning of the Electronic Mail Service.

- **Advanced Criteria**. They are described as those criteria that are necessary but whose implementation is regarded as depending on other aspects apart from the technical ones.

Each criterion is identified with a name, the associated recommendation and its justification. The document contains seven basic criteria and six advanced criteria. Additionally, due to the relevance of the issue, some recommendations to reduce SPAM traffic have been added to the document.

Basic Criteria

1.- Servers Administration

Recommendation: Identify and, if possible, administrate all servers that provide incoming mail service within the institution.

This will allow electronic mail service policies adopted within the company to be applied to all servers offering this service and thus achieve a better control over it.

2.- Control of the inbound SMTP (25) port.

Recommendation: Allow the SMTP port 25 for inbound traffic only for recognized institutional mail servers.

It is necessary to control port 25 in the communications equipment of the institutional network in order to guarantee that only those authorized servers can offer mail service to the institution. By doing so, you can control that the mail server is complying with the service policies established by the institution in terms of security, privacy, levels of service, etc. Control of port 25 is carried out by applying filters to the institution’s border routers, i.e. the routers interconnecting the institution with its external connection providers.

3.- Disable “O pen-relay”

Recommendation: There must not be any institutional mail server acting as Open-Relay.

A server must process only those mails whose senders or recipients are local users. Otherwise, it could happen that the resources of this server are used to send mails from improper users such as mass mails, mails with improper content, etc.

The implementation of a server without “O pen-Relay” will depend on the mail server application used, but in general terms it is necessary to generate a list of all authorized domains and IP addresses of the hosts that can send mail through this MTA. Additionally, all permitted domains will have to make use of MX registers in the DNS.

4.- Inverse Resolution of Names.

Recommendation: All mail servers must have inverse resolution in the DNS.

RFC 1912 – Common DNS Operational and Configuration Errors.
RFC3172 "Ma nagement Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("a rpa").

It is important to point up that currently many Internet relays do not accept traffic from servers that do not have this basic identification.

5.- Statistics

Recommendation: Activate the recollection of SMTP transactions in the mail servers and store the information for a minimum period of thirty days.

Having information about the transactions carried out through mail servers makes it possible to identify possible problems or anomalous behavior of the service. It is also important to have the necessary information to solve possible complaints, either from internal users or operators from other institutions. It must be mentioned that nowadays some instances of investigation at penal level are demanded from institutions, which makes it relevant to have suitable information on the transactions carried out by institutional servers.

6.- Institutional Regulations of the Service

Recommendation: Write a document defining the policies of the electronic mail service offered by the institution and distribute it among the entire institutional community.

Include in the document aspects such as:

- Responsibilities of the Service
- Access model (pop, imap, http)
- Antivirus policy
- AntiSpam policy
- Log policy
- Routing policy: input and output
- Maximum capacity allowed in mailboxes (if there is a limit)
- Mailbox cleaning and elimination policies
- Policy for guest users
- Points of contact: postmaster,abuse@dominio.tld

This document is very important since it regulates the correct functioning of the service and clearly limits the responsibilities of the technicians managing the service.

7.- Points of contact.

Recommendation: It is obligatory to have and maintain addresses for abuse@, postmaster@ incident management support for institutional domains. It is also necessary to keep updated the contact data in WHOIS in our IP ranges.

In Internet, it is standard practice to address complaints over improper behavior using electronic mail to abuse and postmaster mailboxes. Therefore it is fundamental to keep them updated and assign resources for their revision. Consult RFC822 (6.3), RFC2821 (4.5.1) and RFC1123 (5.2.7).

At academic network level there are technical forums devoted to electronic mail service and it is also a good practice to participate in them. At Latin American level there is hermes@reuna.cl. For further information visit http://hermes.reuna.cl

Advanced Criteria

1.- Control of the outbound SMTP port (25)

Recommendation: Allow outbound port 25 (SMTP) only for recognized institutional mail servers.

By following this recommendation it can be guaranteed that electronic mails are always delivered by the institutional servers and not directly by a user or an unauthorized server.

2.- Outbound mail routing

Recommendation: Enable port 587 between users and the institutional mail server instead of port 25.

In order to improve the quality of the electronic mail service offered to users of the institution, it is advisable to use port 587 to route mail towards the Web as indicated in the RFC-2476. At present many institutions use port 25 for this routing. Using port 587 makes it possible to separate the policies of incoming mail from other servers from those policies related to clients. In addition, in order to enhance security it is suggested to introduce authentication in this port 587 as indicated by RFC-2554.

Mail clients of each user will have to modify their configuration in order to send external mail through port 587, implementing the authentication options present in all common mail programs.

3. - Protection of institutional domains

Recommendation: configure the servers to avoid falsification of institutional domains.

It is advisable to implement techniques that make it possible to send mail with institutional domains only from our networks, avoiding thus the spoofing of the domain. In order to achieve this we can:

- Configure the main mail server so that it can only route mails with domain in MAIL FROM corresponding to our institution.
- Define SPF or DKIM registers to declare to the rest of Internet an association between our domains and the institutional servers.

4.- Antivirus for the Institutional mail Service

Recommendation: Install an Antivirus service for the institution's incoming mails.

This makes it possible to improve the security guarantees of the users' mailboxes. It does not imply that users' PC's are not equipped with a personal and updated Antivirus.
Consider also that since many of the messages with viruses are worms and therefore come from spoofed senders, the Antivirus installed will have to be configured to avoid sending replies to the sender and thus increasing the problem.

5.- Time zones

Recommendation: Synchronize institutional mail servers through the NTP protocol using a server from the zone, preferably from the academic world of each country or another country offering it. Some academic NTP servers are:

Argentina: ntp.retina.ar
Brazil:
Spain: ntp.rediris.es

Correct labeling of the time zone in the incoming/outgoing mail servers for messages that are processed, as well as for traces stored in log files, allows a better follow-up to the processing of messages carried out by institutional servers and a better correlation of the information among the servers involved in the service.

6.- Monitoring of the outgoing SMTP traffic

Recommendation: Monitor, as much in real time as possible, the institution's outbound SMTP traffic.

This way mail Service administrators can identify anomalous traffic from a user, such as traffic containing 'malware'. This can happen when an institution's PC is affected by some sort of 'malware' that incorporates an SMTP engine with the objective of propagating a virus, Spam, etc. In order to detect those PC's affected it is very useful to collaborate with other universities or web operators that can inform about anomalous traffic. Notices received through abuse or postmaster mailboxes, and what is declared in the 'whois' of the domains is also useful to detect this kind of traffic.

If we detect or are informed that one of our institution's IP's is emitting non-permitted traffic it will have to be immediately disconnected from the Web.

Appendix 1: ‘A nti-spam Criteria”

Although the adoption of the basic and advanced recommendations is in itself a measure that helps to stop SPAM mail, due to the relevance of the issue we have decided to incorporate this appendix with some specific criteria on the subject.

1. Use blocking lists through DNS (DNSbl): SpamHaus, VIRBL…

2. Demand inverse resolution from the IP’s of servers that establish a connection with our equipment.

3. If possible perform SPF/DKIM/CSV checks.

4. Exclusively accept SMTP transactions whose HELO is an existing domain.

5. In the MAIL FROM: Exclusively accept existing domains.

7. Apply criteria of content and origin filter. This policy must be agreed upon, if possible, or at least widely informed to the community of users so that they are familiar with the criteria that will be used in the filters and can, in turn, feed back administrators of the electronic mail services.

8. Black Lists.

    1. Keep a local version of the Black List with the domains and addresses that are recognised as generators of SPAM towards our users.

    2. Configure the external server to look up RBL’s (Real Time Blackhole Lists)

    3. Configure the external server to look up DUL’s (Dial Up Lists)

9. Do not publish explicit email addresses in web sites.

10. Discussion lists. Develop closed discussion lists, i.e. lists in which people’s inscription is previously authorized by the system administrator.

11. Implement flow control by means of Greylisting.