Network Working Group
Internet-Draft
Expires: June 2004

C. Kularski
Highland School
of Technology

Category: Informational
January 2004

Compound Procedures for SPAM Control

draft-kularski-spam-spamreduce-06.txt

Status of this Memo

Abstract

This document gives instructions for implementing a mail system that will reduce the amount of SPAM received by the end users. The instructions specify disposable and single-purpose mailboxes that will allow for the source of SPAM to be easily identified.

Copyright Notice

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [i].

1. Introduction
   The procedures outlined in this document require an SMTP implementation that is capable of handling custom addressing schemes required by this document. The SMTP service itself should remain in compliance with all standards and specifications.

   This document is NOT a guaranteed solution to SPAM, as of this documentÆs creation no technology existed that would eliminate SPAM completely. This document contains possible solutions that can reduce SPAM, if you are creative with implementing the solutions you will be more successful in reducing SPAM.

2. Address Structuring Considerations
   The procedures in this document are easiest to implement using a sub-domain for each user, such as "user.example.net". The sub-domain SHOULD NOT be defined explicitly, it should be assigned as a wildcard (*) Mail Exchanger RR. If you have a large number of users it will be more efficient to use the dotted or hyphened nomenclature specified in item 3.

3. To avoid DNS issues completely you can use a dotted (.) or hyphenated naming structure before the "at" (@) symbol. The more creative you are with the design of your address schema the fewer SPAM messages your domain is likely to receive.

4. Email Addresses
   There are three main classifications of email address which must be defined.

   Addresses for Automated and Non-Trusted Sources û This set of addresses is defined by the user. There MUST be a way for the user to easily change his/her list of available addresses quickly and easily. The user will need the ability to add and delete addresses from the list. The user will assign a unique address to each non-trusted email source. If the source misuses the address, then the address can be disposed of by deleting it from the list. Mail received by these addresses should be deposited in the userÆs primary mailbox. If a user needs an excessive amount of non-trusted source address a wildcard address can be used for this purpose (with the ability to kill abused addresses), but it is not recommended.

   Address for Personal Communication û The address for personal communication is a single email address defined by either the user or the administrator. This address will most likely be the one used as the primary mailbox for the user. The user should give this address only to human sources that are unlikely to spread the address. This address is optional.

Addresses for Common Services, Roles and Functions û Addresses defined by RFC 2142[ii] should be directed to the mailbox of the appropriate function on the primary domain (example: abuse@user.example.net is delivered to abuse@example.net).

5. Considerations for Each Address Type
   Each address type has its own special needs for them to be used to their full potential and to allow the least amount of SPAM in.

   Addresses for Automated and Non-Trusted Sources û These addresses MUST be unique to each source. Mail for these addresses can be filtered to add an additional level of SPAM elimination, but the nature of these addresses will significantly reduce the amount of SPAM received.

   Address for Personal Communication û This address should be protected in several ways. First, the address should not be widely distributed and should NEVER be used for newsgroups, web pages or any purpose where it will be publicly viewable. Additionally the mailbox SHOULD use a whitelist (and blacklist) system to authorize senders. Score-based SPAM detection systems can also be reliable in "weeding out" SPAM from this box. Failing to adequately protect this address will defeat the purpose of this document.

   Addresses for Common Roles, Services and Functions û due to the nature of these addresses they should not be extremely restrictive, but due to the nature of SPAM attacks some protection is advisable.

6. Possible Special Addresses
   In addition to the addresses for non-trusted sources temporary addresses that expire after a certain amount of time has elapsed can be used for situations where SPAM is imminent, such as newsgroup communication.

7. Address Examples
   Sub-domain Non-trusted source û source@user.example.net
   Dotted-user Non-trusted source û source.user@example.net
   Hyphened-user Non-trusted source û source-user@example.net
   Sub-domain Personal û user@user.example.net
   Dotted (or Hyphened) Personal û user@example.net

Security Considerations

The information in this document introduces no Security Concerns.

References

i Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

ii Crocker, D., "Mailbox Names for Common Roles, Services and Functions", RFC 2142, May 1997

Author's Addresses

Curtis M. Kularski
219 Best St
Bessemer City, NC 28016-9330
United States
Phone: +1 (704) 629-2498
Email: spamreducedraft@curtis.kularski.us

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.