

Network Working Group
Internet-Draft
Expires: March 2004

C. Kularski
Highland School
of Technology
September 2003

Category: Informational

Compound Procedures for SPAM Control
draft-kularski-spam-spamreduce-04.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

Abstract

This document describes procedures that can be put into place to significantly reduce the amount of SPAM received by a user. The procedures are implemented on the SMTP server.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

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 a complex SMTP implementation that is capable of handling the addressing schemes required by this document. The SMTP service itself should remain in compliance with all standards and specifications.

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.

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 you are likely to receive.

3. Email Addresses

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

Addresses for Automated and Non-Trusted Sources - 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 user's 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 - 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.

Addresses for Common Services, Roles and Functions - Addresses defined by RFC 2142[iii] 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).

4. 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 - 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 - 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 can use a whitelist (and blacklist) system to authorize senders or you can use a score-based SPAM detection system.

Addresses for Common Roles, Services and Functions - 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.

5. 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.

6. Address Examples

Sub-domain Non-trusted source - spammer@user.example.net

Dotted-user Non-trusted source - spammer.user@example.net

Hyphened-user Non-trusted source - spammer-user@example.net

Sub-domain Personal - user@user.example.net

Dotted (or Hyphened) Personal - 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: curtis@kularski.net

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are

included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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