Individual submission
Internet-Draft
Intended status: BCP
Expires: June 8, 2012

M. Kucherawy
Cloudmark, Inc.
December 6, 2011

# Best Current Practices for Email Greylisting
# draft-ietf-appsawg-greylisting-00

## Abstract

This memo describes best current practices for the art of email greylisting, the practice of providing temporarily degraded service to unknown email clients as an anti-abuse mechanism.

## Status of This Memo

This Internet-Draft will expire on June 8, 2012.

## Copyright Notice

Table of Contents

1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . 3
2. Definitions . . . . . . . . . . . . . . . . . . . . . . . . . 3
2.1. Keywords . . . . . . . . . . . . . . . . . . . . . . . . 3
2.2. E-Mail Architecture Terminology . . . . . . . . . . . . . . 3
3. Benefits and Costs . . . . . . . . . . . . . . . . . . . . . 3
4. Connection-Level Greylisting . . . . . . . . . . . . . . . . 4
5. SMTP HELO/EHLO Greylisting . . . . . . . . . . . . . . . . . 4
6. SMTP MAIL Greylisting . . . . . . . . . . . . . . . . . . . . 4
7. SMTP RCPT Greylisting . . . . . . . . . . . . . . . . . . . . 4
8. SMTP DATA Greylisting . . . . . . . . . . . . . . . . . . . . 4
9. Deciding Who Is Affected . . . . . . . . . . . . . . . . . . 4
10. Effects on Clients . . . . . . . . . . . . . . . . . . . . . 4
11. Recommendations . . . . . . . . . . . . . . . . . . . . . . . 5
12. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 5
13. Security Considerations . . . . . . . . . . . . . . . . . . . 5
14. References . . . . . . . . . . . . . . . . . . . . . . . . . 5
14.1. Normative References . . . . . . . . . . . . . . . . . . 5
14.2. Informative References . . . . . . . . . . . . . . . . . 6
Appendix A. Acknowledgments . . . . . . . . . . . . . . . . . . . 6

## 1. Introduction

There are many techniques in use for dealing with email abuse. One is a set of techniques known as "greylisting". Broadly, this refers to any degradation of service for an unknown or suspect source, over a period of time. The narrow use of the term refers to generation of an SMTP temporary failure reply code for traffic from such sources.

There are diverse implementations of this general technique, and, predictably therefore, some blurred terminology.

This memo documents common greylisting techniques and discusses their benefits and costs. It also defines terminology to enable clear distinction and discussion of these techniques.

## 2. Definitions

### 2.1. Keywords

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 [KEYWORDS].

### 2.2. E-Mail Architecture Terminology

Readers should be familiar with the material and terminology discussed in [MAIL] and [EMAIL-ARCH].

## 3. Benefits and Costs

This section will discuss the benefits and also the costs (resources and impacts on generals ervice) of the various implementations.

Discuss failure modes, including:

- all retries fail

- retries go to a different server that doesn't know about previous attempts

- retries come from a different client than earlier ones

- for systems that use body hashes, the retries aren't the same as the previous attempts

## 4. Connection-Level Greylisting

This section will talk about greylisting applied at the time of decision about whether or not to accept a new connection, even before SMTP begins to take place.

## 5. SMTP HELO/EHLO Greylisting

This section will talk about greylisting applied within the [SMTP] session at the HELO/EHLO phase.

## 6. SMTP MAIL Greylisting

This section will talk about greylisting applied within the [SMTP] session at the MAIL FROM phase.

## 7. SMTP RCPT Greylisting

This section will talk about greylisting applied within the [SMTP] session at the RCPT TO phase.

## 8. SMTP DATA Greylisting

This section will talk about greylisting applied within the [SMTP] session at the DATA phase.

Some implementations do filtering here because there are clients that don't bother checking SMTP reply codes to commands other than DATA.

## 9. Deciding Who Is Affected

This section will discuss how it is decided whether or not a particular client session, or specific message, will be selected for greylisting. Discuss selection criteria, e.g., {IP} vs. {IP, from, to}.

## 10. Effects on Clients

This section will discuss the behaviours of SMTP clients when greylisting is in effect, such as:

- very long retry times

- aggressive retries can hit rate limits

- incorrect handling of greylisting replies (e.g., treat 4xx like 5xx)

- retries may change envelope sender

## 11. Recommendations

This section will provide some general recommendations about when and how to deploy greylisting in various conceptual environments.

Some points to discuss:

- logging of a greylisting server vs. one not greylisting can be a good measure of how effective it is

- can also compare greylisting results to DNSBLs and content filtering

- greylisting is more expensive than not greylisting

- greylisting delays legitimate mail, and can cause conversations to arrive out of order

- time limits for greylisting

- special actions to take if the same message is retried before the time limit expires

- recommended termiantion methods (421 vs. 4xx)

- affects/requirements on MXes other than the lowest

- ability to share information between servers

## 12. IANA Considerations

No actions are requested of IANA in this memo.

## 13. Security Considerations

This section discusses potential security issues related to greylisting.

## 14. References

### 14.1. Normative References

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

## 14.2. Informative References

[EMAIL-ARCH] Crocker, D., "Internet Mail Architecture", RFC 5598, October 2008.

[MAIL] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[SMTP] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

## Appendix A. Acknowledgments

The author wishes to acknowledge Mike Adkins, Steve Atkins, Dave Crocker, Peter J. Holzer, John Levine, Jose-Marcio Martins da Cruz, S. Moonesamy, Jordan Rosenwald, Gregory Shapiro, and Joe Sniderman for their contributions to this memo.

## Author's Address

Murray S. Kucherawy
Cloudmark, Inc.
128 King St., 2nd Floor
San Francisco, CA 94107
US

Phone: +1 415 946 3800
EMail: msk@cloudmark.com