Network Working Group
Internet Draft
<draft-hutzler-spamops-06>
Intended status: Best Current Practice
Expires: November 2007

C. Hutzler
D. Crocker
Brandenburg InternetWorking
P. Resnick
QUALCOMM Incorporated
R. Sanders
E. Allman
Sendmail, Inc.
May 2007

Email Submission: Access and Accountability

draft-hutzler-spamops-06

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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/1id-abstracts.txt>.

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

This Internet-Draft will expire in November 2007.

Copyright Notice

Abstract

Email has become a popular distribution service for a variety of socially unacceptable, mass-effect purposes. The most obvious ones include spam and worms. This note recommends conventions for the operation of email submission and transport services between independent operators, such as enterprises and Internet Service Providers. Its goal is to improve lines of accountability for controlling abusive uses of the Internet mail service. Consequently the document offers recommendations for constructive operational policies between independent operators of email transmission services.

With the recent advent of email authentication technologies aimed at providing assurances and traceability between internetworked networks, the authors recognized that the initial submission of a message became the weakest link. Consequently, the document offers recommendations for constructive operational policies for the first step of email sending, the submission (or posting) of email into the transmission network. Relaying and delivery entail policies that occur subsequent to submission and are outside the scope of this document.

The document seeks BCP status. Comments and discussion of this document should be addressed to the ietf-smtp@imc.org mailing list.

Table of Contents

1. Introduction

The very characteristics that make email such a convenient communications medium -- its near ubiquity, rapid delivery and low cost -- have made it a fertile ground for the distribution of unwanted or malicious content. Spam, fraud and worms have become a serious problem, threatening the viability of email and costing end users and providers millions of dollars in damages and lost productivity. In recent years, independent operators including enterprises and ISPs have turned to a number of different technologies and procedures, in an attempt to combat these problems, with varying effect and with vastly different impacts on users and on the Internet mail infrastructure.

Email will often travel between multiple independent providers of email transmission services, en route to its final destination. They will generally have no prior arrangement with one another and may employ different rules on the transmission. It is therefore difficult both to debug problems that occur in mail transmission and to assign accountability if undesired or malicious mail is injected into the Internet mail infrastructure.

A wide variety of email authentication technologies has been developed, and more are under development. They provide some accountability and traceability between disparate networks. This document aims to build on these technologies by exploring best practices for authenticating and authorizing the first step of an email's delivery from MUA to MSA, otherwise known as submission. Without strong practices on email submission, the authentication technologies provide limited benefit.

This document specifies operational policies to be used for the first step of email sending, the submission (or posting from an MUA to an MSA as defined below) of email into the transmission service. These policies will permit continued, smooth operation of Internet email, with controls added to improve accountability. Relaying and delivering employ policies that occur after submission and are outside the scope of this document. The policies listed here are appropriate for operators of all sizes and may be implemented by operators independently, without regard for whether the other side of an email exchange has implemented them.

It is important to note that the adoption of these policies alone will not solve the problems of spam and other undesirable email. However they provide a useful step in clarifying lines of accountability and interoperability between operators. This helps raise the bar against abusers, and provides a foundation for additional tools to preserve the utility of the Internet email infrastructure.

This document does not delve into other anti-spam operational issues such as standards for rejection of email. The authors note that this would be a very valuable effort to undertake and suggest that additional work under another BCP document should be embarked upon.

2. Terminology

The Internet email architecture distinguishes four message-handling components:

- Mail User Agents (MUAs)
- Mail Submission Agents (MSAs)
- Mail Transfer Agents (MTAs)
- Mail Delivery Agents (MDAs)

At the origination end, an MUA works on behalf of end users to create a message and perform initial "submission" into the transmission infrastructure, via an MSA. An MSA accepts the message submission, performs any necessary preprocessing on the message and relays the message to an MTA for transmission. MTAs “relay” messages to other MTAs, in a sequence reaching a destination MDA that, in turn, “delivers” the email to the recipient's inbox. The inbox is part of the recipient-side MUA that works on behalf of the end-user to process received mail.

These architectural components are often compressed, such as having the same software do MSA, MTA and MDA functions. However the requirements for each of these components of the architecture are becoming more extensive, so that their software and even physical platform separation is increasingly common

Note: 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 [RFC2119].

3. Submission, Relaying, Delivery

The MSA, MTA and MDA functions used to be considered as the same set of functions. This has been reflected in the history of Internet mail by having MSA, MTA and MDA transfers all be performed with SMTP [RFC2821] [RFC0821], over TCP Port 25. Internet mail permits email to be exchanged with no prior arrangement. Hence Port 25 exchanges occur without sender authentication. That is, the confirmed identity of the originator of the message is not necessarily known by the relaying MTAs or the MDA.

It is important to distinguish MUA-to-MSA email submission, versus MTA relaying, versus the final MTA-to-MDA transmission, prior to MDA- to-MUA delivery. Submission typically does entail a pre-established relationship between the user of the client and operator of the server; equally, the MDA can determine that it will be affecting final delivery and has an existing relationship with the recipient. That is, MSAs and MDAs can take advantage of having prior relationships with users, in order to constrain their transfer activities.

Specifically, an MSA can choose to reject all postings from MUAs for which it has no existing relationship. Similarly, an MDA can choose to reject all mail to recipients for which that MDA has no arrangement to perform delivery. Indeed, both of these policies are already in common practice.

3.1 Best Practices for Submission Operation

Submission Port Availability:

> If external submissions are supported -- that is, from outside a site's administrative domain -- then the domain's MSAs MUST support the SUBMISSION port 587 [RFC4409]. It is also suggested that operators standardize on the SUBMISSION port for both external AND LOCAL users for simplicity.

Submission Port Use:

> MUAs SHOULD use the SUBMISSION port for message submission.

Submission Authentication:

> MSAs MUST perform authentication on the identity asserted during all mail transactions on the SUBMISSION port, even for a message having a RCPT TO address that would not cause the message to be relayed outside of the local administrative environment.

Submission Authorization:

> Operators of MSAs MUST perform authorization of the authenticated identity, for the operations performed during mail submission and based on an existing relationship with the submitting entity. This requirement applies to all mail submission mechanisms (MUA to MSA).

Submission Accountability after Submission:

> Once a message has been submitted, the message SHOULD be later traceable by the MSA operator to the authenticated identity of the user who sent the message for a reasonable period of time. Such tracing MAY be based on transactional identifiers stored in the headers (received lines, etc) or other fields in the message. The specific length of time, after message submission, that traceability is supported is not specified here. However issues regarding transit often occur as much as one week after submission.

3.2 Transitioning to Submission Port

In order to promote transition of initial message submission from port 25 to port 587, MSAs SHOULD listen on both ports. MSAs MUST require authentication on port 587 and SHOULD require authentication on port 25. MSAs MAY also listen on other ports. Regardless of the ports on which messages are accepted, MSAs MUST NOT permit relaying of unauthenticated messages to other domains (i.e., they must not be open relays).

As delivered from the factory, MUAs SHOULD attempt to find the best possible submission port from a list of alternatives. That list SHOULD include the SUBMISSION port 587 as well as port 25. The ordering of that list SHOULD try the SUBMISSION port 587 before trying port 25, and MAY try other ports before, between, or after those two ports. Since most MUAs available today do not permit falling back to alternate ports, sites SHOULD pre-configure or encourage their users to connect on the SUBMISSION port 587, assuming that site supports that port.

4. External Submission

An MUA, desiring special services, may need to submit mail across the Internet, rather than to a local MSA, in order to obtain particular services. Examples include active privacy protection against third-party content monitoring and timely processing. Further the privacy requirement might reasonably include protection against monitoring by the operator of the MUA's access network. This requirement creates a challenge for the provider operating the IP network through which the MUA gains access. It makes that provider an involuntary recruit to the task of solving mass-effect email problems: When the MUA participates in a problem that affects large numbers of Internet users, the provider is expected to effect remedies and is often expected to prevent such occurrences.

A proactive technique used by some providers is to block all use of Port 25 SMTP for mail that is being sent outbound, or to automatically redirect this traffic through a local SMTP proxy, except for hosts that are explicitly authorized. This can be problematic for some users, notably legitimate mobile users attempting use their "home" MSA, even though those users might already employ legitimate, Port 25-based authentication.

This document offers no recommendation concerning the blocking of SMTP Port 25 and similar practices for controlling abuse of the standard anonymous mail transfer port. Rather, it pursues the mutually constructive benefit of using the official SUBMISSION Port 587 [RFC4409].

Note: However the authors wish to note that many established practices for controlling abuse of port25, for mail that is being sent outbound, currently exist. These include the proxy of smtp traffic to local hosts for screening combined with various forms of rate limits. The authors suggest that this topic should be addressed in a separate BCP that would benefit the operational communities.

4.1 Best Practices for Support of External Submissions

Open Submission Port:

Access Providers MUST NOT block users from accessing the external Internet using the SUBMISSION port 587 [RFC4409].

Traffic Identification -- External Posting Versus Relaying:

For email being received from outside their local operational environment, email service providers MUST distinguish between mail that will be delivered inside that environment, versus mail that is to be relayed back out to the internet. This allows the MTA to restrict this operation, preventing the problem embodied by "open" relays. Note that there are situations where this may not apply such as secondary MXs and related implementations internal to an operator's network and within their control.

Delivery Authorization:

MDAs MUST NOT accept mail to recipients for which that MDA has no arrangement to perform delivery.

Figure 1 depicts a local user (MUA.l) submitting a message to an MSA (MSA). It also shows a remote user (MUA.r), such as might be in a coffee shop offering "hotspot" wireless access, submitting a message to their "home" MSA via an Authenticated Port 587 transaction.

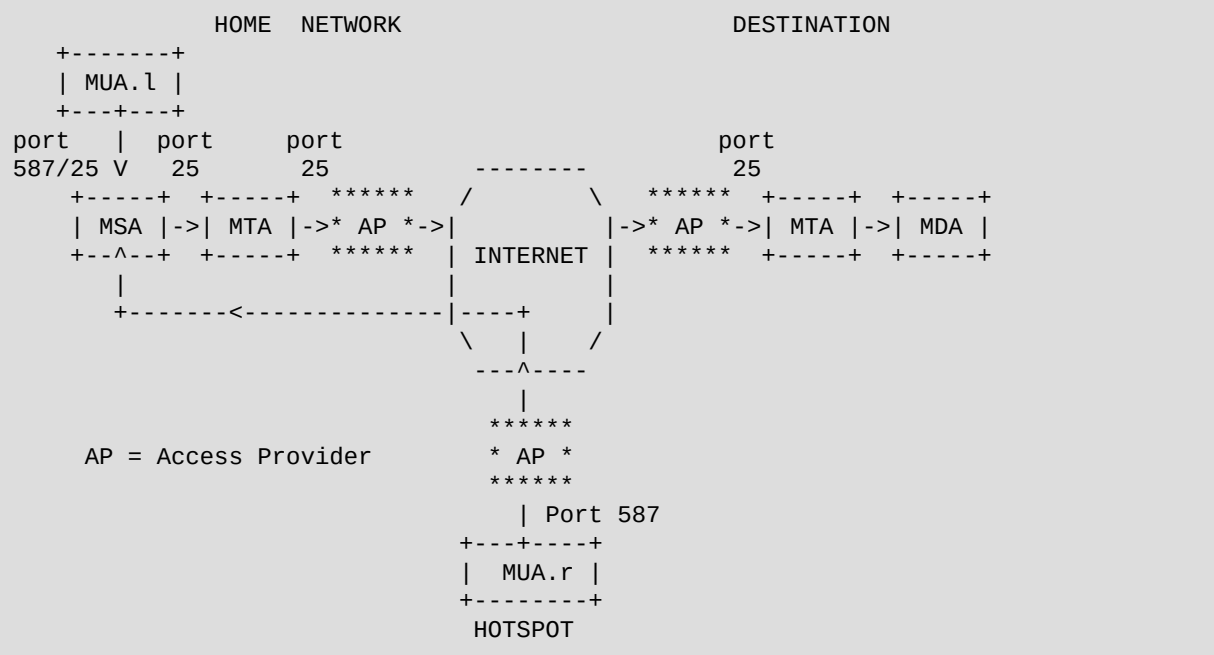

Figure 1: Example of Port 587 Usage Via Internet

5. Message Submission Authentication/Authorization Technologies

There are many competent technologies and standards for authenticating message submissions. Two mechanisms that have been standardized include SMTP AUTH [RFC2554] and TLS [RFC3207]. Depending upon the environment, different mechanisms can be more or less effective and convenient. Organizations SHOULD choose the most secure approaches that are practical.

This document does not provide recommendations on specific security implementations. It simply provides a warning that transmitting user credentials in clear text over insecure networks SHOULD be avoided in all scenarios as this could allow attackers to listen for this traffic and steal account data. In these cases, it is strongly suggested that an appropriate security technology MUST be used.

6. Security Considerations

Email transfer between independent administrations can be the source of large volumes of unwanted email and email containing malicious content designed to attack the recipient's system. This document addresses the requirements and procedures to permit such exchanges while reducing the likelihood that malicious mail will be transmitted.

7. References

7.1 References -- Normative

[RFC0821] Postel, J.B., "Simple Mail Transfer Protocol", STD 10, RFC 821, August 1982.

[RFC2821] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[RFC4409] Gellens, R. and J.C. Klensin, "Message Submission for Mail", RFC 4409, April 2006.

7.2 References -- Informative

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2554] Myers, J., "SMTP Service Extension for Authentication".

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", February 2002.

Authors' Addresses

C. Hutzler
2512 Freetown Drive
Reston, VA 20191
Phone: 703-915-6862
EMail: cdhutzler@aol.com
URI: http://carlhutzler.com/blog/

D. Crocker
Brandenburg InternetWorking
675 Spruce Dr.
Sunnyvale, CA 94086
USA
Phone: +1.408.246.8253
EMail: dcrocker@bbiw.net
URI: http://bbiw.net

P. Resnick
QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA 92121-1714
USA
Phone: +1 858 651 4478
EMail: presnick@qualcomm.com
URI: http://www.qualcomm.com/~presnick/

R. Sanders
Atlanta, GA
USA
Phone:
EMail:
URI:

E. Allman
Sendmail, Inc.
Emeryville, CA
USA
Phone: +1 510 594 5501
EMail: eric+ietf-smtp@sendmail.org

A. Acknowledgments

These recommendations were first formulated during informal discussions among members of Anti-Spam Technical Alliance (ASTA) and some participants from the Internet Research Task Force's Anti-Spam Research Group (ASRG).

Full Copyright Statement

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org[1].

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

[1] mailto:ietf-ipr@ietf.org