Network Working Group
Request for Comments: 5068
BCP: 134
Category: Best Current Practice

C. Hutzler
D. Crocker
Brandenburg InternetWorking
P. Resnick
QUALCOMM Incorporated
E. Allman
Sendmail, Inc.
T. Finch
University of Cambridge Computing Service

November 2007

Email Submission Operations: Access and Accountability Requirements

Status of This Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

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. To this end, this document offers recommendations for constructive operational policies between independent operators of email submission and transmission services.

Email authentication technologies are aimed at providing assurances and traceability between internetworked networks. In many email services, the weakest link in the chain of assurances is initial submission of a message. This document offers recommendations for constructive operational policies for this 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.

Table of Contents

1. Introduction

The very characteristics that make email such a convenient communications medium -- its near ubiquity, rapid delivery, low cost, and support for exchanges without prior arrangement -- 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. The results have been mixed, at best.

En route to its final destination, email will often travel between multiple independent providers of email transmission services. These services 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.

Many email authentication technologies exist. They provide some accountability and traceability between disparate networks. This document aims to build upon the availability of these technologies by exploring best practices for authenticating and authorizing the first step of an email's delivery, from a Mail User Agent (MUA) to a Mail Submission Agent (MSA), known as submission. Without strong practices on email submission, the use of authentication technologies elsewhere in the service provides 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 of networks 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, these policies 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.

NOTE: This document does not delve into other anti-spam operational issues such as standards for rejection of email. The authors note that this could be a valuable effort to undertake and encourage its pursuit.

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.

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

Originally the MSA, MTA, and MDA architectural components were considered to be a single unit. This was reflected in the practice of having MSA, MTA, and MDA transfers all be performed with SMTP [RFC2821] [RFC0821], over TCP port 25. Internet mail permits email to be exchanged without prior arrangement and 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 transition. Submission typically does entail a pre-established relationship between the user of the client and operator of the server; equally, the MDA is performing final delivery and can determine that it 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 it 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]. Operators MAY standardize on the SUBMISSION port for both external AND LOCAL users; this can significantly simplify submission operations.

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 domain.

Submission Authorization:

> An operator of an MSA MUST ensure that the authenticated identity is authorized to submit email, based on an existing relationship between the submitting entity and the operator. This requirement applies to all mail submission mechanisms (MUA to MSA).

Submission Accountability after Submission:

> For a reasonable period of time after submission, the message SHOULD be traceable by the MSA operator to the authenticated identity of the user who sent the message. Such tracing MAY be

based on transactional identifiers stored in the headers (received lines, etc.) or other fields in the message, on audit data stored elsewhere, or on any other mechanism that supports sufficient post-submission accountability. 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.

Note that [RFC3848] defines a means of recording submission-time information in Received header fields. This information can help receive-side analysis software establish a sending MSA's accountability and then make decisions about processing the message.

3.2. Transitioning to Submission Port

In order to promote transition of initial message submission from port 25 to port 587, MSAs MUST listen on port 587 by default and SHOULD have the ability to listen on other ports. MSAs MUST require authentication on port 587 and SHOULD require authentication on any other port used for submission. 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. That is, they must not be open relays.

As a default, MUAs SHOULD attempt to find the best possible submission port from a list of alternatives. The SUBMISSION port 587 SHOULD be placed first in the list. 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 might need to submit mail across the Internet, rather than to a local MSA, in order to obtain particular services from its home site. Examples include active privacy protection against third-party content monitoring, timely processing, and being subject to the most appropriate authentication and accountability protocols. 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 to 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 or 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: Many established practices for controlling abuse of port 25, for mail that is being sent outbound, currently do exist. These include the proxy of SMTP traffic to local hosts for screening, combined with various forms of rate limits. The authors suggest that a separate document on this topic would benefit the email operations community.

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 (MSA) Versus Relaying (MX):

When receiving email from outside their local operational environment, email service providers MUST distinguish between unauthenticated email addressed to local domains (MX traffic) versus submission-related authenticated email that can be addressed anywhere (MSA traffic). This allows the MTA to restrict relaying operations, and thereby prevent "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.

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. The figure shows the alternative of using port 587 or port 25 within the MSA's network. This document makes no recommendations about the use

of port 25 for submission. The diagram merely seeks to note that it is in common use and to acknowledge that port 25 can be used with sufficient accountability within an organization's network.

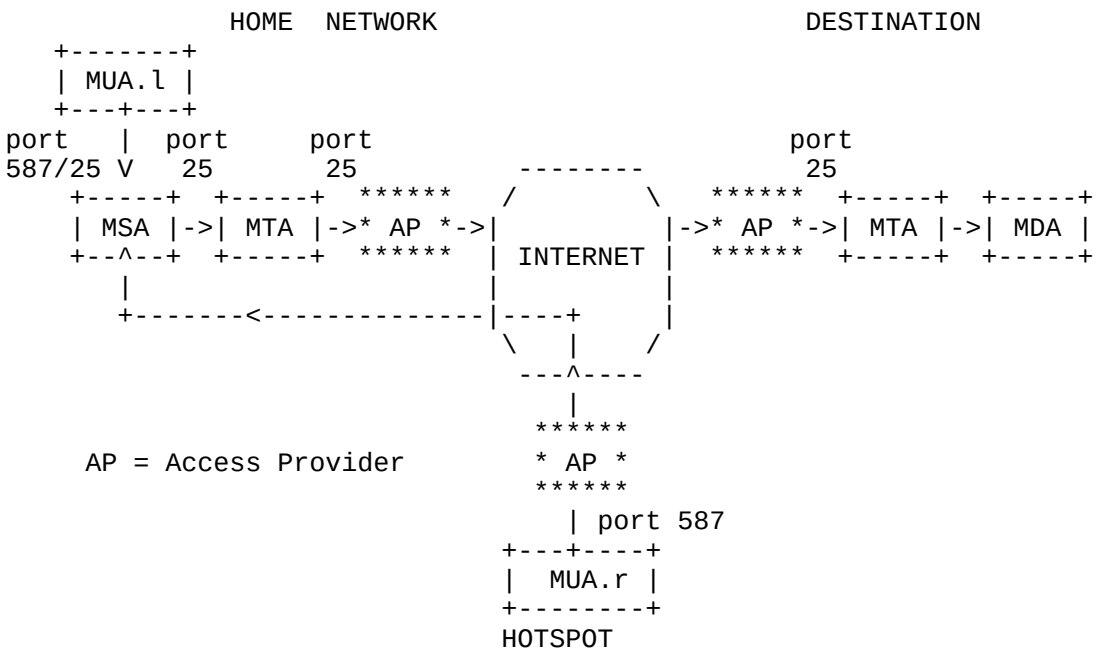

Figure 1: Example of Port 587 Usage via Internet

5. Message Submission Authentication/Authorization Technologies

There are many competent technologies and standards for authenticating message submissions. Two component mechanisms that have been standardized include SMTP AUTH [RFC4954] and TLS [RFC3207]. Depending upon the environment, different mechanisms can be more or less effective and convenient. Mechanisms might also have to be used in combination with each other to make a secure system. 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. Normative References

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

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

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

7.2. Informative References

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

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, February 2002.

[RFC3848] Newman, C., "ESMTP and LMTP Transmission Types Registration", RFC 3848, July 2005.

[RFC4954] Siemborski, R., Ed. and A. Melnikov, Ed., "SMTP Service Extension for Authentication", RFC 4954, July 2007.

Appendix 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).

Later reviews and suggestions were provided by: M. Allman, L.H. Aestrand, N. Borenstein, S. Bortzmeyer, K. Chon, R. Clayton, B. Cole, W. Dnes, V. Duchovni, E. Edelstein, F. Ellermann, M. Elvey, J.D. Falk, N. Freed, J. Glube, A. Herzberg, J. Klensin, J. Levine, S. Moonesamy, K. Moore, R. Nelson, C. Newman, C. O'Malley, S. Ramasubramanian, R. Rognlie, J. St. Sauver, W. Schlitt, B. Shein, B. Sullivan.

Authors' Addresses

Carl Hutzler
2512 Freetown Drive
Reston, VA 20191

Phone: 703-915-6862
EMail: cdhutzler@aol.com
URI: http://carlhutzler.com/blog/

Dave Crocker
Brandenburg InternetWorking
675 Spruce Dr.
Sunnyvale, CA 94086
USA

Phone: +1.408.246.8253
EMail: dcrocker@bbiw.net
URI: http://bbiw.net

Peter 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/

Eric Allman
Sendmail, Inc.
6745 Christie Ave., Suite 350
Emeryville, CA
USA

Phone: +1 510 594 5501
EMail: eric+ietf-smtp@sendmail.org

Tony Finch
University of Cambridge Computing Service
New Museums Site
Pembroke Street
Cambridge CB2 3QH
ENGLAND

Phone: +44 797 040 1426
EMail: dot@dotat.at
URI: http://dotat.at/

Full Copyright Statement

Intellectual Property