Network Working Group
Internet-Draft
Updates: 5321, 4409 (if approved)
Intended status: Informational
Expires: May 5, 2016

S. Josefsson

L. Nordberg
DFRI

November 2, 2015

# Improving Privacy for the email "Received" Header
draft-josefsson-email-received-privacy-01

## Abstract

The email "Received" header raises a privacy concern with email routing. This document discusses the problem and describes a solution that relevant Message Transfer Agents (MTAs) and Mail Submission Agents (MSAs) may adopt.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on May 5, 2016.

Table of Contents



## 1. Introduction

As mentioned in RFC 7624 section 3.3.4 [RFC7624], the Simple Mail Transfer Protocol (SMTP) [RFC5321] requires that each successive SMTP relay adds a "Received" header to the mail headers. The purpose of these headers is to enable audit of mail transmission, and perhaps to distinguish between regular mail and spam. An attacker that can observe sufficient email traffic can regularly update the mapping between public IP addresses and individual email identities. Even if the SMTP traffic was encrypted on submission and relaying, the attacker can still receive a copy of public mailing lists.

While not mentioned in RFC 7624, the Received header is used for loop detection, as discussed in section 6.3 of SMTP [RFC5321].

To give an example of a privacy violation, consider the following scenario. When SMTP is used for message submission [RFC4409], the SMTP server accepting the email from the user MUA will add a Received header that will record the IP address of the user's host. When the email is circulated further in the Internet environment, possibly ending up publicly archives, it will be possible to read this Received header. This allows an attacker to learn the IP address of the host used by the individual who sent the email. This consitutes a privacy violation. The knowledge of the IP address of the user may be used to gather additional information about the user, or to simplify direct attacks against the host of the user.

Privacy violations may also happen when adding additional Received headers after an email has been delivered to the MX for the destination domain, where anyone who can observe the Received header

can learn additional information about the internal network topology of a single organization. The privacy relevance of this information depends on each organization.





There may be other situations where adding Received headers would leak unintended information to an observing party. For example, an organization may use different SMTP relays depending on the category of a customer. By knowing the mapping between SMTP relay and customer category, an observing party would learn the customer category for the organization.

The privacy problem we are interested in resolving is the part of an SMTP agent (be it an MTA or an MSA) that persistently records the IP address of the client in the Received header.

The purpose of this document is to propose a mechanism that implementers and operators of SMTP agents may adopt to mitigate the privacy violation.

For ease of reference, the syntax of the Received header is defined in RFC 5322 section 3.6.7 [RFC5322] and the SMTP protocol requirement to add them is described in RFC 5321 section 4.4 [RFC5321].

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 [RFC2119].

## 2. Privacy-sensitive Received header Convention

The "from clause" of the Received header MUST NOT be added by SMTP entities concerned with the privacy of their clients.

With "from clause", we intend what in [RFC2821] is denoted as "From-domain" in the ABNF. To illustrate what is intended, consider the following Received header that were added by a MSA and thus leaked the then-current IP address of the submitter's host.

```
Received: from latte.josefsson.org ([155.4.17.2])
 by duva.sjd.se (8.14.4/8.14.4/Debian-4) with ESMTP id t9QFWqNO022103
 (version=TLSv1/SSLv3 cipher=AES128-GCM-SHA256 bits=128 verify=NOT);
```

Mon, 26 Oct 2015 16:32:53 +0100

The from clause is the part of the header that reads "from latte.josefsson.org ([155.4.17.2])".

## 3. Acknowledgements

The following individuals provided valuable feedback: Philipp Winter, Georg Koppen, Jacob Appelbaum, Christian Huitema, Ned Freed, John Levine





## 4. Security Considerations

This document resolves a privacy concern with the Received header. The privacy concern is discussed as a security consideration in section 7.6 of SMTP [RFC5321] however that document does not provide any mechanism for implementers who are concerned about the problem to "opt out".

## 5. IANA Considerations

IANA is adviced to add this document to the Reference column of the "Permanent Message Header Field Names" registry for "Received".

## 6. References

### 6.1. Normative References

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

[RFC4409] Gellens, R. and J. Klensin, "Message Submission for Mail", RFC 4409, DOI 10.17487/RFC4409, April 2006, <http://www.rfc-editor.org/info/rfc4409>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <http://www.rfc-editor.org/info/rfc5321>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI

10.17487/RFC5322, October 2008,
<http://www.rfc-editor.org/info/rfc5322>.

## 6.2. Informative References

[RFC2821] Klensin, J., Ed., "Simple Mail Transfer Protocol", RFC 2821, DOI 10.17487/RFC2821, April 2001, <http://www.rfc-editor.org/info/rfc2821>.

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <http://www.rfc-editor.org/info/rfc7624>.





## Appendix A. Copying conditions



## Authors' Addresses

Simon Josefsson

Email: simon@josefsson.org

Linus Nordberg
DFRI

Email: linus@dfri.se