

Individual submission
Internet-Draft
Updates: [5965](#), [6591](#) (if approved)
Intended status: Standards Track
Expires: November 8, 2012

R. Clayton
University of Cambridge
M. Kucherawy
Cloudmark, Inc.
May 7, 2012

Source Ports in ARF Reports
draft-kucherawy-marf-source-ports-03

Abstract

This document defines an additional header field for use in Abuse Reporting Format reports to permit the identification of the source port of the connection involved in an abuse incident.

This document updates [RFC5965](#) and [RFC6591](#).

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 November 8, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as

described in the Simplified BSD License.

Table of Contents

| | | |
|-----------------------------|--|-------------------|
| 1. | Introduction | 3 |
| 2. | Keywords | 3 |
| 3. | Source-Port Field Definition | 3 |
| 4. | Time Accuracy | 3 |
| 5. | IANA Considerations | 4 |
| 6. | Security Considerations | 4 |
| 7. | References | 4 |
| 7.1. | Normative References | 4 |
| 7.2. | Informative References | 5 |
| Appendix A. | Acknowledgements | 5 |

1. Introduction

[ARF] defined the Abuse Reporting Format, an extensible message format for Email Feedback Reports. These reports are used to report incidents of email abuse. ARF was extended by [[AUTHFAILURE-REPORT](#)] to enable reporting of email authentication failures. These specifications provided for the source IP address to be included in a report. As explained in [[LOG](#)], the deployment of IP address sharing techniques requires the source port values to be included in reports if unambiguous identification of the origin of abuse is to be achieved.

This document defines an ARF reporting field to contain this information and provides guidance for its use.

2. 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](#)].

3. Source-Port Field Definition

A new ARF header field called "Source-Port" is defined. When present in a report, it MUST contain the TCP source port matching the "Source-IP" field in the same report, thereby describing completely the origin of the abuse incident.

Per, [[ABNF](#)], the formal syntax is:

```
source-port = "Source-Port:" [CFWS] 1*DIGIT [CFWS] CRLF
```

"CFWS" is imported from [[MAIL](#)].

When any report is generated that includes the "Source-IP" reporting field (see Section 3.2 of [[ARF](#)]), this field SHOULD also be present, unless the port number is unavailable.

Use of this field is RECOMMENDED for reports generated per [[AUTHFAILURE-REPORT](#)] (see [Section 3.1](#) of that document).

4. Time Accuracy

[LOG] underscores the importance of accurate clocks when generating reports that include source port information because of the fact that source ports can be recycled very quickly in Internet Service Provider environments. The same considerations described there apply here.

Report generators that include an Arrival-Date report field MAY choose to express the value of that date in Universal Coordinated Time (UTC) to enable simpler correlation with local records at sites that are following the provisions of [[LOG](#)].

[5.](#) IANA Considerations

IANA is requested to add the following entry to the Feedback Report Header Fields registry:

Field Name: Source-Port

Description: TCP source port from which the reported connection originated

Multiple Appearances: No

Related Feedback-Type: any

Reference: [this document]

Status: current

[6.](#) Security Considerations

This extension introduces no new security considerations not already covered in [[ARF](#)].

Some security considerations related to the general topic of source port logging can be found in [[LOG](#)].

[7.](#) References

[7.1.](#) Normative References

- | | |
|----------------------|--|
| [ABNF] | Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234 , January 2008. |
| [ARF] | Shafranovich, Y., Levine, J., and M. Kucherawy, "An Extensible Format for Email Feedback Reports", RFC 5965 , August 2010. |
| [AUTHFAILURE-REPORT] | Fontana, H., "Authentication Failure Reporting using the Abuse Report Format", RFC 6591 , April 2012. |
| [KEYWORDS] | Bradner, S., "Key words for use in RFCs to |

Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

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

7.2. Informative References

[LOG] Durand, A., Gashinsky, I., Lee, D., and S. Sheppard, "Logging Recommendations for Internet-Facing Servers", [RFC 6302](#), June 2011.

Appendix A. Acknowledgements

The authors wish to acknowledge the following for their review and constructive criticism of this proposal: Steve Atkins, Scott Kitterman, John Levine, and Doug Otis.

The idea for this work originated within the Messaging Anti-Abuse Working Group (MAAWG).

Authors' Addresses

Richard Clayton
University of Cambridge
Computer Laboratory
JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom

Phone: +44 1223 763570
EMail: richard.clayton@cl.cam.ac.uk

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

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

