Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 5, 2011

J. Falk
Return Path

March 4, 2011

Redaction of Potentially Sensitive Data from Mail Abuse Reports
draft-jdfalk-marf-redaction-00

Abstract

Email messages often contain information which might be considered private or sensitive, per either regulation or social norms. When such a message becomes the subject of a report intended to be shared with other entities, the report generator may wish to redact or elide the sensitive portions of the message. This memo suggests one method for doing so effectively.

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 September 5, 2011.

Copyright Notice

described in the Simplified BSD License.

Table of Contents

1. Introduction

[ARF] defines a message format for sending reports of abuse in the messaging infrastructure, with an eye toward automating both the generating and consumption of those reports.

For privacy considerations it might be the policy of a report generator to redact, or obscure, portions of the report that might identify an end user that caused the report to be generated. Precisely how this is done is unspecified in [ARF] as it will generally be a matter of local policy. That specification does admonish generators against being too over-zealous with this practice, as obscuring too much data makes the report inactionable.

Previous redaction practices, such as replacing local-parts of addresses with a uniform string like "xxxxxxxx", often frustrated any kind of prioritizing or grouping of reports.

Generally, it is assumed that the recipient fields of a message, when copied into a report, are to be obscured to protect the identify of an end user that submitted a complaint about a message. However, it is also presumed that other data will be left intact, data that could be correlated against logs to determine the source of the message that drew a complaint.

2. Recommended Practice

To enable correlation of reports that might refer to a common but anonymous source, the following redaction practice is recommended:

1. Select an arbitrary string that will be used by an Administrative Domain (ADMD) that generates reports. This string will not be changed except according to a key rotation policy or similar. Call this the "redaction key".
2. Identify string(s) (such as local-parts of email addresses) in a message that need to be redacted. Call this the "private data".
3. Construct a new string that is a copy of the redaction key with the private data concatenated to it.
4. Compute a digest of that string with any hashing/digest algorithm such as SHA1.
5. Encode that hash with the base64 algorithm as defined in [MIME].
6. Replace the private data with the encoded hash when generating the report.

This has the effect of obscuring the data in an irreversible way but still allows the report recipient to observe that numerous reports are about one particular end user. Such detection enables the

receiver to prioritize its reactions based on problems that appear to be focused on specific end users that may be under attack.

3. Security and Privacy Considerations

Security issues with respect to these reports are found in [ARF].

While the method of redaction described in this document may somewhat reduce the likelihood of some types of private data from leaking between Administrative Domains, it is extremely unlikely that report generation software could ever be created to recognize all of the different ways that private information may be expressed through human written language. If further protections are required, implementors may wish to consider establishing legal contracts or other non-technology-based agreements between the relevant entities.

4. References

[ARF] Shafranovich, Y., Levine, J., and M. Kucherawy, "An Extensible Format for Email Feedback Reports", RFC 5965, August 2010.

[MIME] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

Author's Address

J.D. Falk
Return Path
100 Mathilda Place, Suite 100
Sunnyvale, CA 94086
US

Email: ietf@cybernothing.org
URI: http://www.returnpath.net/