DKIM Working Group
Internet-Draft
Intended status: Informational
Expires: February 18, 2011

M. Kucherawy
Cloudmark
August 17, 2010

RFC4871 Implementation Report
draft-ietf-dkim-implementation-report-00

Abstract

This document contains an implementation report for the IESG covering DKIM in support of the advancement of that specification along the Standards Track.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

[DKIM], published in May 2007, has reached a level of maturity sufficient to consider its advancement along the standards track. Enclosed is a summary of collected interoperability data provided from sources that are aggregating such information as well as from a more formal DKIM interoperability event that took place in October 2007.

2. Definitions

Various terms specific to email are used in this document. Their definitions and further discussion can be found in [EMAIL-ARCH].

3. DKIM Interoperability Event

In October 2007, Alt-N Technologies of Dallas, Texas hosted an interoperability and testing event at their headquarters. Twenty organizations sent engineers and their various DKIM implementations to connect to a private internal network and exchange test messages and tabulate observed results.

3.1. Participants

The interoperability event included participants from all of the following organizations: Alt-N Technologies, AOL, AT&T Inc., Bizanga Ltd., Brandenburg InternetWorking, Brandmail Solutions, ColdSpark, Constant Contact, Inc., DKIMproxy, Domain Assurance Council, Google Inc., ICONIX Inc., Internet Initiative Japan (IIJ), Ironport Systems, Message Systems, Port25 Solutions, Postfix, Sendmail, Inc., StrongMail Systems, and Yahoo! Inc. Most of the participants traveled to Dallas and participated in person, but a few operated remotely.

Nearly all of the implementations were based on disjoint code development projects. A few were based on a common open source base project.

3.2. Testing Methodology

Participants were encouraged before the event to craft a set of test messages meant to exercise their own implementations as well as those of the other participants, both in terms of successful verifications as well as some expected to fail. Some test cases were developed with the intent of confounding verifiers that may not have implemented the [ABNF] of [DKIM] correctly.

The participants set up Mail Transfer Agents (MTAs) equipped with their own DKIM signing and verifying modules, and their own tools to generate mail to be signed along with tools to analyze the results post-verification. They then sent their own batteries of test messages, looking for both expected and unexpected failures in response. Some implementations included "auto-responders" that would reply with verification results, while others simply collected the results that would then be shared manually.

3.3. Observations

All of the implementations implemented all of the required portions of [DKIM] in terms of both signature and key features. Most of the implementations implemented all of the optional features of both signatures and keys. There were no notable or common exceptions.

The interoperability testing was largely successful. As might be expected, there were many verification false negatives or false positives that were the result of bugs in corner cases of some of the implementations presented for testing. In such cases the developers were able to identify the issue as resulting from their own mis-reading of the specification and not an error in the specification itself.

Several of the failures did occur as a result of specification ambiguities. The participants discussed each of these in turn and were able to come to consensus on how they believed the specification should be changed to resolve them.

3.4. Results

The handful of interoperability issues described above that referred to weaknesses or ambiguities in [DKIM] resulted in several errata being opened via the RFC Editor web site. These are being addressed in an RFC4871bis draft effort that is now starting from within the DKIM working group.

4. Collected DKIM Interoperability and Use Data

Several implementations are collecting private data about DKIM use, signature survivability, which properties of the base specification are observed in public use, etc. This section includes collection methods and summary reports provided by those implementations.

4.1. The OpenDKIM Project

The OpenDKIM Project is an open source project providing a DKIM support library, an email filter for use with MTAs, and a set of tools to assist with deployment of DKIM.

4.1.1. Details

Recent releases have included an optional feature to record statistics about messages with and without DKIM signatures. Sites enabling this feature can choose to share the data with the project's development team as part of this interoperability report work. The data can be anonymized to conceal the sending domain and client IP addresses, though these data are passed through a one-way hash to enable collation of data from common sources.

4.1.2. Results

At the time of writing of this document, the results of this effort are as follows:

Reporting Hosts: 11 individual MTAs representing seven distinct ADMDs

Total Messages: 111101

Signatures: 80984 messages (72.9%) were not signed; 29663 (26.7%) had one signature; 419 (0.3%) had two signatures; the remainder (less than 0.04%) had more

Signing Algorithms: 58.5% of signatures used "rsa-sha1", while the balance used "rsa-sha256"

Header Canonicalization Algorithms: 31.3% of signatures used "simple", while the balance used "relaxed"

Body Canonicalization Algorithms: 38.6% of signatures used "simple", while the balance used "relaxed"

Keys in Test Mode: 46% of keys retrieved from the DNS were tagged as being in test mode

Keys with Syntax Errors: 0.1% of keys retrieved from the DNS had syntax errors

Missing Keys: 1.4% of signatures received referenced keys that were not found in the DNS

Optional Signature Tags: Of the optional signature tags supported by the base specification, "t=" was seen 45.7% of the time (0.4% of which included timestamps in the future, even after forgiving some clock drift); "x=" was seen 4.6% of the time; "l=" was seen 3.3% of the time; "z=" was seen 3.0% of the time.

Body Length Limits: Of the signatures for which "l=" was used, 76.1% of them had the body extended after signing.

Signature Pass Rates: Overall, 72.7% of observed signatures were successfully verified.

Pass Rates for Non-List Mail: Where "list mail" is defined as any mail not bearing one of the header fields defined in [LIST-ID] or in [LIST-URLS], or a "Precedence: list" field, selecting only for mail that is not list mail revealed a successful verification rate of 92.5%; selecting only for list mail produced a 54.3% success rate.

Author vs. Third-Party: 75.2% of the signatures observed were author signatures, meaning the "d=" value in the signature matched the domain found in the From: header field. The remainder, therefore, were third-party signatures.

4.1.3. Conclusions

The results of the OpenDKIM work are updated constantly as more data feeds come online and more data are reported. Based on the data available at the time of writing, some conclusions are possible.

At least some implementations of all of the optional signature features, all of the canonicalization combinations and all of the signing algorithms are in general use. None of the features had zero use counts.

The current collection implementation did not collect data about optional features of keys that are in use. A future version will address this.

Overall signature pass rates are generally quite high, except for cases where the mail passes through a mailing list. In that case almost half of the signatures are invalidated. (Earlier snapshots of data in this effort showed this figure to be even higher.) It follows that for DKIM to be successful, increased co-operation with MLMs is desirable. The working group has already started work on an informational draft discussing use of DKIM with respect to MLMs, and it would seem these data support the importance of completing that work.

4.2. Other Collected Data

[Summaries of data collected and reported by other sources can go here.]

5. Security Considerations

This document is an implementation report and thus has no security considerations.

6. References

6.1. Normative References

[DKIM] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", RFC 4871, May 2007.

6.2. Informative References

[ABNF] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 5234, January 2008.

[EMAIL-ARCH]
Crocker, D., "Internet Mail Architecture", RFC 5598, July 2009.

[LIST-ID] Chandhok, R. and G. Wenger, "List-Id: A Structured Field and Namespace for the Identification of Mailing Lists", RFC 2919, March 2001.

[LIST-URLS]
Neufeld, G. and J. Baer, "The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields", RFC 2369, July 1998.

Appendix A. Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this document: [names]

The working group expresses its thanks to Alt-N Technologies for graciously hosting the 2007 DKIM interoperability event.

Author's Address

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

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