Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 3, 2014

J. Levine
Taughannock Networks

May 2, 2014

A DKIM Profile to Enable Message Forwarding
draft-levine-may-forward-01

Abstract

Some mail systems have been observed to use authentication schemes the domain name in the From: header as a security key, in combination with DKIM, an approach works poorly in connection with forwarders that edit messages. This document describes a profile of DKIM intended to improve interoperation of DKIM with such schemes.

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 3, 2014.

Table of Contents

1. Introduction

Some mail systems have been observed to use authentication schemes the domain name in the From: header as a security key, in combination with DKIM [RFC6376], an approach works poorly in connection with forwarders that edit messages. If forwarders edit messages in ways typical of mailing lists, such as adding subject line tags and messages headers or footers, existing DKIM signatures are no longer valid, and such authentication schemes fail. This has been observed to cause rejection of messages that the recipients want to receive and other undesirable effects.

Some approaches for modifying mail software to work around this issue are described in [RFC6377], but due do a combination of non-adoption and changing security models, they are not adequate.

This document describes a restricted DKIM profile, intended to create DKIM signatures that will survive message modifications, and a DKIM signature tag intended to identify such signatures for the benefit of anti-spam and other assessment schemes.

2. Definitions

2.1. 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 [RFC2119].

3. A DKIM Profile for May-Forward

A "may-forward" DKIM signature is an ordinary DKIM signature that meets the following criteria:

1. The only signed header is From. That is, the signature header contains "h=from".

2. The responsible SDID is the domain in the address in the From: header, that is, the signature header contains "d=fromdomain" where "fromdimain is that domain.

3. The signature SHOULD use relaxed header canonicalization, that is, the signature header contains "c=relaxed/relaxed" or "c=relaxed/simple".

4. The message body is unsigned, that is, the signature header contains "l=0".

5. The signature header contains the new may-forward tag "mf=targetdomain", described below.

Other fields in the DKIM signature header such as t= and z= are created as normal. The signer SHOULD also apply conventional DKIM signature(s) without the may-forward tag.

A forwarder SHOULD preserve may-forward signatures with d= domains that match the From: domain, even if it normally deletes incoming DKIM signatures.

4. The May-Forward Tag

The new "mf=targetdomain" tag indicates that a DKIM signature is intended to survive forwarding. The "targetdomain" is the domain name that is expected to do the forwarding. While it has no specific meaning in the context of DKIM signature validation, it is intended for use by higher level assessment software to aid in their evaluation of a message. If a message also has a DKIM signature with a d= domain that matches the targetdomain in an mf tag, (a "forwarding signature") that indicates that the message has been forwarded as anticipated.

A sender that expects a message to be forwarded might put both a conventional DKIM signature and a may-forward signature. The forwarder uses the conventional signature to assess the message, edits the message, and then signs the outgoing message with its own signature. Subsequent recipients observe both the forwarder's signature and the may-forward with an mf tag that matches the other

signature, and use either or both to assess the message. If a message arrives with a may-forward signature but no forwarding signature, the recipient would ignore the may-forward signature or assign it lower weight since the message has not been forwarded as expected.

5. IANA Considerations

IANA is requested to add an entry to the "DKIM-Signature Tag Specifications" registry.

TYPE	REFERENCE	STATUS
mf	(this document)	active

Table 1: DKIM-Signature Tag Specifications additions

6. Security Considerations

DKIM was designed to provide assurances that a message with a valid signature was received in essentially the same form that it was sent. This profile deliberately circumvents that design, to create a loophole for messages intended to be forwarded by entities that edit the message. It opens up a variety of obvious replay attacks that may or may not be important depending on both the selection of target domains for messages to be forwarded, and the behavior of forwarders that receive messages with may-forward signatures.

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.

[RFC6376] Crocker, D., Hansen, T., and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, September 2011.

7.2. Informative References

[RFC6377] Kucherawy, M., "DomainKeys Identified Mail (DKIM) and Mailing Lists", BCP 167, RFC 6377, September 2011.

Author's Address

John Levine
Taughannock Networks
PO Box 727
Trumansburg, NY 14886

Phone: +1 831 480 2300
Email: standards@taugh.com
URI: http://jl.ly