DKIM Working Group
Internet-Draft
Intended status: Informational
Expires: February 11, 2007

M. Thomas
Cisco Systems

August 10, 2006

Requirements for a DKIM Signing Practices Protocol
draft-ietf-dkim-ssp-requirements-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on February 11, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

DomainKeys Identified Mail [DKIM] provides a cryptographic mechanism for domains to assert responsibility for the messages they sign. A related mechanism would allow an administrator ot publish various statements about their email accountability practices. This draft defines the requirement for this additional mechanism.

Table of Contents

1. Preface

The purpose of this draft is get out into the open a range of issues related to the perceived need for a signing practices information service primarily focused on DKIM. This document is intended to document well-agreed upon problems and requirements, in addition to less well-agreed upon requirements in an attempt to capture the issue as well as generalize the requirement as much as possible. These latter requirements will be noted as "[PROVISIONAL]" to indicate that there is not yet solid consensus, or that the problem is not well understood. A winnowing process is envisioned where the more difficult and/or speculative problems/requirement will be eliminated unless concrete problems with proven constituencies can be demonstrated, along with reasonable plausibility that they do not contradict more well agreed upon requirements.

2. Definitions

- Domain Holder: the entity that ultimately controls the contents of the DNS subtree starting at the domain, either directly or by delegation via NS records it controls.

- First Party Address: For DKIM, a first party address is defined to be the RFC2822.From address in the message header; a first party address is also known as a Author address

- First Party Signature: For DKIM, a first party signature is a valid signature where the domain tag (d=) matches (as defined in [DKIM]) the first party address

- Third Party Signature: For DKIM, a third party signature is a valid signature that does not qualify as a First Party Signature. Note that a DKIM third party signature does is not required to correspond to a third party address such as Sender or Listid, etc.

- DKIM Signer Complete: the state where the domain holder believes that all legitimate mail purportedly from the domain was sent with a valid DKIM signature.

- The Protocol: in this document, The Protocol is used as placeholder for a protocol that will meet the requirements set in this draft.

3. Introduction

The DomainKeys Identified Mail working group is chartered to create a base signing mechanism for email. This work is contained in draft-ietf-dkim-base-04.txt. In addition there are two other documents draft-ietf-dkim-overview-00.txt and draft-ietf-dkim-threats-03.txt which give an overview and a threat analysis of the chartered work. This draft reflects the requirements for the last part of the chartered work to define a protocol to publish DKIM signing practices.

While the base signing document defines a mechanism for signing and verifying DKIM signatures, there has been a great deal of interest in a signing practices protocol. The most pressing case seems to be the bid down attack inherent with almost all systems that allow optional authentication: how does a receiver know whether or not it should expect a message to contain authentication information? For email this is an especially difficult problem since generally there is no a priori knowledge of other domains so the safe assumption is the lowest common denominator which is no authentication at all. Thus a protocol needs to be developed which can allow a DKIM message verifier to determine the DKIM posture of the domain for messages it receives which arrive without a valid DKIM signature.

This draft is organized into two main sections: a Usage Scenario section which attempts to describe some common usage scenarios that DKIM is likely to be deployed in and the problems that are not solved by DKIM alone. The second is the Requirements that arise because of those usage scenarios, in addition more basic protocol requirements.

4. Use Scenarios

The email world is a diverse world with many deployment scenarios. This section tries to outline some usage scenarios that it is expected that DKIM signing/verifying will take place in, and how a new protocol might be helpful to clarify the relevance of DKIM signed mail.

4.1. Scenario 1: Bigbank.example.com

There seems to be a class of mail -- mostly transactional mail from high value domains -- that are the target of phishing attacks. In particular, the phishing scams forge the RFC2822.From address in addition to spoofing much of the content to trick unsuspecting users into revealing sensitive information. Domain holders sending this kind of mail would like the ability to guarantee that their mail is always from them. The first step is, of course, to use DKIM-base to sign all of their outgoing mail so that a receiver can make a positive determination that the mail is from the domain holder in question.

The problem with this scenario is that a receiver in the general case doesn't know what the practices are for a given domain, or what their expectations are for unsigned mail. An information service which allowed a receiver to query for those practices and expectations could be useful to close the gap where an attacker merely sends unsigned mail to exploit a bid down attack. It is assumed that receivers would use this information to treat such questionable mail with prejudice.

Note that for the foreseeable future, DKIM signature breakage for unrestricted use patterns (ie with users and especially where users are members of mailing lists) will likely suffer occassional damage in transit. While probably not a large percentage of total traffic, the kind (quality) of breakage may be significant for certain usage patterns. As such, this scenario defines a more limited situation where the risk of a legitimate piece of mail being mislabeled as unsigned outweights the risk of illegitimate mail being delivered in the eyes of the sender.

1. A purportedly sends to B with a missing or broken DKIM signature from A

2. B would like to know whether that is an acceptable state of affairs.

4.2. Scenario 2: DKIM Signing Complete

After auditing their outgoing mail and deploying DKIM signing for all of their legitimate outgoing mail, a domain could be said to be DKIM signing complete. That is, the domain has to the best of its ability insured that all mail legitimately purporting to have come from that domain contained a valid DKIM signature. Given the likelihood of signature damage in the current mail infrastructure as noted above, a domain can fit the DKIM signing complete scenario without wanting to take the risks associated with the more narrow scope of use in the previous scenario. A receiver, on the other hand, may be able to take advantage of the knowledge the domain's practice of signing all mail in order to use it to bias filters against the unexpected arrival of a piece of unsigned or damaged in transit mail.

4.3. Scenario 3: Outsourced First Party Signing

Many domains do not run their own mail infrastructure, or may outsource parts of it to third parties. It is desirable for a domain holder to have the ability to be able to enumerate a list of domains that should be treated as equivalent to a first party signature from the domain holder itself. One obvious use scenario is a domain holder for a small domain that needs to have the ability for their outgoing ISP to sign all of their mail on behalf of the domain holder. Other use scenarios include outsourced bulk mail for marketing campaigns, as well as outsourcing various business functions such as insurance benefits, etc.

That said, DKIM uses DNS to store selectors. Thus there is always the ability for a domain holder to delegate all or parts of the _domainkey subdomain to a third party of the domain holder's choosing. That is, the domain holder can always set a NS record for _domainkey.example.com to, say, an email provider who manages that namespace. There is also the ability for the domain holder to partition its namespace into subdomains to further constrain how third parties. For example, a domain holder could delegate only _domainkey.benefits.example.com to a third party to further constrain the third party to only be able to sign messages on behalf of the benefits subdomain.

There have been concerns expressed about how well this would scale when the third party is, say, a large ISP that signs for thousands of domains. There has been concern about how well this would work for multiple delegations. Lastly, using NS delegations requires that the signer actively cooperate with the domain for whom it is signing. That is, it requires that the signer actively manage the _domainkey delegation for the domain holder. A domain holder would not, for example, be able to make a statement that ISP.com signing on its

behalf was acceptable without ISP.com's cooperation. This by extension also applies to other third parties that a domain might like to effectively "whitelist" such as mailing lists that re-sign mail that the domain holder holds in esteem.

5. Requirements

This section defines the requirements for The Protocol. As with most requirements drafts, these requirements define the MINIMUM requirements that a candidate protocol must provide. It should also be noted that The Protocol must fulfill all of the requirements.

[Informative Note: it's not clear to the author that all of the provisional requirements can fulfill the harder requirements. If this is determined to be true, the provisional requirement should either be dropped or the harder requirements revised]

5.1. Discovery Requirements

1. Discovery mechanism MUST be rooted in DNS.

2. Discovery mechanism MUST converge in a deterministic number of exchanges.

   [Informative Note: this, for all intents and purposes is a prohibition on anything that might produce loops; also though "deterministic" doesn't specify how many exchanges, the expectation is "few".]

3. Discovery mechanism MUST NOT overload semantics of existing DNS resource records where name space collisions are possible.

5.2. Transport requirements

1. Widespread deployment of the transport layer would be highly desirable, especially if riding on top of a true transport layer (eg, TCP, UDP).

2. A low-cost query/response in terms of latency time and the number of packets involved is highly desirable.

3. If the infrastructure doesn't provide caching (ala DNS), the records retrieved will need time-to-live values to allow querying verifiers to maintain their own caches. Existing caching infrastructure is, however, highly desirable.

4. Multiple, geographically and topologically diverse servers must be supported for high availability

5.3. Practice and Expectation Requirements

In this section, a Practice is defined as a true statement according to the domain holder of its intended externally viewable behavior. An Expectation combines with a Practice to convey what the domain holder considers the likely outcome of the survivability of the Practice at a receiver. For example, a Practice that X is true when it leaves the domain, and an Expectation that it will|will-not|may|may-not remain true for some/all receivers.

1. The Protocol MUST be able to make Practices and Expectation assertions about the RFC2822.From address in the context of DKIM. The Protocol will not make assertions about other addresses for DKIM at this time.

2. The Protocol MUST be able to publish a Practice that the domain doesn't send mail.

3. The Protocol MUST be able to publish a Practice that the domain's signing behavior is "DKIM Signing Complete"

4. The Protocol MUST be able to publish an Expectation that a verifiable First Party DKIM Signature should be expected on receipt of a message.

   [Informative Note: the DKIM Signing Complete Practice seems to be a pre-requisite for this Expectation]

5. [PROVISIONAL] A domain MUST be able to delegate responsibility for signing its messages to a non-related domain in such a way that it does not require active participation by the non-related domain. That is, the published information MUST have a way to specify the domains that are allowed to sign on its behalf.

6. Practices and Expectations MUST be presented as an information service from the sender to be consumed as an added factor to the receiver's local policy. In particular a Practice or Expectation MUST NOT specify any particular disposition stance that the receiver should follow.

7. If the Discovery process would be shortened by publication of a "null" practice, the protocol SHOULD provide a mechanism to publish such a practice.

   [INFORMATIVE NOTE: there seems to be widespread consensus that a "neutral" or "I sign some mail" practice is useless to receivers. However, a null practice may help to cut short the policy lookup mechanism if it's published, and if that

the case it seems worthwhile. Also, a null policy may have some forensic utility, such as gaging the number of domains considering/using DKIM for example.]

8. The Protocol is not required to publish a Practice of any/all unreleated third parties that MUST NOT sign on the domain holder's behalf.

   [INFORMATIVE NOTE: this is essentially saying that the protocol doesn't have to concern itself with being a blacklist repository.]

9. The Protocol MUST NOT be required to be invoked if a valid first party signatures is found.

10. [PROVISIONAL] A domain holder MUST be able to publish a Practice which enumerates the acceptable cryptographic algorithms for signatures purportedly from that domain.

    [INFORMATIVE NOTE: this is to counter a bid down attack; some comments indicated that this need only be done if the algorithm was considered suspect by the receiver; I'm not sure that I've captured that nuance correctly]

5.4. Extensibility and Forward Compatibilty Requirements

1. The Protocol MUST NOT extend to any other than DKIM for email at this time.

2. The Protocol MUST be able to add new Practices and Expectations within the existing discovery/transport/practices in a backward compatible fashion.

3. [PROVISIONAL] The Protocol MUST be able to extend for new protocols signed by DKIM

4. [PROVISIONAL] The Protocol MUST be able to extend for protocols other than DKIM

6. Security Requirements

1. Minimize DoS potential: The Protocol for a high-value domain is potentially a high-value DoS target, especially since the unavailability of The Protocol's record could make unsigned messages less suspicious.

2. Amplification Attacks: The Protocol MUST NOT make highly leveraged amplification or make-work attacks possible. In particular any amplification must be order of a constant.

3. Authenticity: The Protocol MUST have the ability for a domain holder to provide The Protocol's data such that a receiver can determine that it is authentically from the domain holder with a large degree of certainty. The Protocol may provide means which provide less certainty in trade off for ease of deployment.

7. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

8. Security Considerations

This draft defines requirements for a new protocol and the security related requirements are defined above. There is an expectation that The Protocol will not always be required to have source authentication of the practices information which is noteworthy.

9. Acknowledgements

free to good home

10. References

10.1. Normative References

10.2. Informative References

Author's Address

Michael Thomas
Cisco Systems
606 Sanchez St
San Francisco, California 94114
USA

Phone: +1-408-525-5386
Fax: +1-408-525-5386
Email: mat@cisco.com

Full Copyright Statement

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).