Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 27, 2014

S. Rose
NIST

September 23, 2013

Using Secure DNS to Assert S/MIME Usage
draft-srose-smimelock-00

Abstract

This draft defines and discusses the use of a new DNS resource record (RR) type to address S/MIME downgrade attacks. The SMIMELOCK RR allows a domain to convey general message security policy. Primarily, this RR allows the domain owner to advertise a policy that all legitimate messages from this domain will be signed by a verifiable certificate.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft will expire on March 27, 2014.

Copyright Notice

Table of Contents

1. Introduction

1.1. Overview

While it is difficult to change the content of an S/MIME signed message without detection, it is not difficult to remove the S/MIME wrapper and change the content of the resulting unsigned message. If the recipient of the altered message did not know that the message originally contained a digital signature then there would be no indication of foul play.

Likewise, attackers masquerading as valid users can send messages purporting to be from those users. Without digital signatures it is difficult for the recipient to know whether or not the message was legitimate.

The introduction of a new DNS record type, SMIMELOCK, provides a DNSSEC [RFC4033], [RFC4034], and [RFC4035] authenticated mechanism to enable MUAs to determine whether a message sender's policy was to digitally sign all messages before sending. Based on SMIMELOCK query results, each domain is assigned one of two policy states: MUST SIGN or POLICY UNKNOWN.

To reduce unnecessary DNS queries, the SMIMELOCK policy applies to all users within a domain (the "right-hand side" of the email address, called the "domain" in RFC 5322 [RFC5322]).

This proposal is produced in conjunction with a DANE/SMIME proposal, but the two MAY be used independently. The lock concept is based on the RLOCK record proposed in draft-gersch-grow-revdns-bgp-02. [I-D.gersch-grow-revdns-bgp]

1.2. Scope

We limit the scope of this internet draft to associating S/MIME message signing policy with all users of a given domain. S/MIME enveloped- only (encrypted) messages provide no data integrity or source authentication. If a message was wrongly sent in plaintext then the damage was already done once it was sent. Conversely, if a message is received without a signature then damage occurs only when trust or lack of trust is incorrectly assigned to the message.

SMIMELOCK results SHOULD be used only by MUAs processing received messages. MUAs preparing messages to send SHOULD NOT base message signature decisions on SMIMELOCK results.

This proposal is limited to authenticating message contents and end-entity senders. It is distinct and complementary to existing

processes (like SPF [RFC4408] or DKIM [RFC6376] and ADSP[RFC5617]).

2. The SMIMELOCK Resource Record

The SMIMELOCK DNS resource record (RR) is used to convey a domain's message signing policy to MUAs processing received messages. This provides the ability for MUAs to identify and flag messages in violation of their originating domain's advertised signing policy.

The type value for the SMIMELOCK RR type is to be assigned.

The SMIMELOCK RR is class independent.

The SMIMELOCK RR has no special TTL requirements.

A zone MUST NOT contain more than one SMIMELOCK record for the same owner name.

2.1. The SMIMELOCK RDATA Format

The RDATA of an SMIMELOCK consists of a single octet. The values have the following meanings:

```
    0: reserved
    1: ALL (interpreted as MUST SIGN all messages)
```

Any result other than ALL is interpreted as POLICY UNKNOWN

Other values (i.e. policies) could be added in the future, but conditional policies are discouraged as they increase the opportunity for downgrade attacks.

2.2. SMIMELOCK RR Example

The SMIMELOCK policy applies to all users in a domain (where domain refers to the "right hand side" of an email address). For example, to request an SMIMELOCK RR applicable to "alice@example.com", the QNAME would be "example.com". The query result would apply equally to any message originator from the example domain (e.g. "bob@example.com", "chuck@example.com", etc.). A wildcard RR will extend the policy to cover fictitious subdomains (e.g. frank@fake.example.com") and individual hostnames in the zone.

SMIMELOCK resource records for the example.com zone:

```
            example.com.    IN SMIMELOCK  ALL
            *.example.com.  IN SMIMELOCK  ALL
```

3. Use of SMIMELOCK Resource Records in S/MIME

Use of SMIMELOCK is opt-in by the sending domain and by the receiving MUA. If a domain owner creates an SMIMELOCK RR, there is no guarantee that MUAs will check it.

3.1. DNSSEC considerations

Responses for SMIMELOCK RR's SHOULD be disregarded unless the RRSet passes DNSSEC validity checks. Criteria in [RFC6698] section 4.1 MAY be used. The absence of a valid SMIMELOCK result (either NOERROR/ NODATA RCODE or SMIMELOCK RR with unknown RDATA values) SHOULD be interpreted as POLICY UNKNOWN by the client.

3.2. Signature Checks

A compliant MUA MUST check SMIMELOCK status for the domain of each message received unless the message is S/MIME signed. MUST SIGN status MAY be cached and re-used up to the life of the SMIMELOCK RR TTL value. POLICY UNKNOWN status MAY be cached by the MUA for up to 24 hours before issuing a new SMIMELOCK request for the domain.

A compliant MUA MUST flag SMIMELOCK signature policy violations (i.e. unsigned messages originating from domains with MUST SIGN policy). Unsigned messages from domains with MUST SIGN policy MUST NOT be presented to the recipient as free from errors. Unsigned messages from domains with MUST SIGN policy MAY be presented to the recipient as having failed signature verification.

3.3. Status Checks

Since this process fails silently, active checks SHOULD be implemented by administrators of domains and MUAs.

4. IANA Considerations

4.1. SMIMELOCK RRType

This document uses a new DNS RR type, SMIMELOCK whose value [TBD] has been allocated by IANA from the Resource Record (RR) TYPEs subregistry of the Domain Name System (DNS) Parameters registry.

4.2. SMIMELOCK Policy Statement Types

This document creates a new registry, "SMIMELOCK Policy Statement Types". The registry policy is "Specification Required". The initial entries in the registry are:

Value	Short description	Reference
0	Reserved	[this doc]
1	ALL	[this doc]
2-255	Unassigned	

Applications to the registry can request specific values that have yet to be assigned.

5. Security Considerations

There is an acknowledged shortcoming in this current proposal that an attacker need only block or alter the DNS response to disable the SMIMELOCK capability. However, the ability to affect DNS (signed with DNSSEC) for a recipient's MUA is considerably more difficult than sending a spoofed email to the recipient.

This draft also seeks input on the best way to convey signature policy violations to message recipients. It is possible that a poor implementation could make matters worse. If a MUA treats a signature policy violation as a failed signature verification, then it SHOULD NOT present views of the data in which the message appears to be signed unless it is clear that the signature verification failed.

6. Acknowledgements

Todd Larsen, Doug Montgomery, and Stephen Nightingale contributed technical ideas and support to this document.

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.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012.

7.2. Informative References

[I-D.gersch-grow-revdns-bgp] Gersch, J., Massey, D., Olschanowsky, C., and L. Zhang, "DNS Resource Records for Authorized Routing Information", draft-gersch-grow-revdns-bgp-02 (work in progress), February 2013.

[RFC4408] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408, April 2006.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[RFC5617] Allman, E., Fenton, J., Delany, M., and J. Levine, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)", RFC 5617, August 2009.

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

Author's Address

Scott Rose
NIST
100 Bureau Dr.
Gaithersburg, MD 20899
USA

Phone: +1-301-975-8439
EMail: scott.rose@nist.gov