Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 29, 2012

M. Miller
P. Saint-Andre
Cisco Systems, Inc.

June 27, 2012

Using DNS Security Extensions (DNSSEC) and DNS-based Authentication of Named Entities (DANE) as a Prooftype for XMPP Domain Name Associations

draft-miller-xmpp-dnssec-prooftype-02

Abstract

This document defines a prooftype that uses DNS-based Authentication of Named Entities (DANE) for associating a domain name with an XML stream in the Extensible Messaging and Presence Protocol (XMPP). It also defines a method that uses DNS Security (DNSSEC) for securely delegating a source domain to a derived domain in XMPP.

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 December 29, 2012.

Copyright Notice

Table of Contents

1. Introduction

The [XMPP-DNA] specification defines a framework for secure delegation and authenticated domain name associations (DNA) in the Extensible Messaging and Presence Protocol (XMPP). This document defines a a secure delegation method that uses DNS Security (DNSSEC) [RFC4033] in conjuction with the standard DNS SRV records [RFC2782] employed in domain name resolution in XMPP, with the result that a client or peer server that inititates an XMPP stream can legitimately treat a derived domain as a reference identifier during stream negotiation. This document also defines a prooftype for DNA that uses DNS-based Authentication of Named Entities [DANE] to verify TLS certificates containing source domains or derived domains during stream negotiation.

2. Terminology

This document inherits XMPP-related terminology from [RFC6120], DNS-related terminology from [RFC1034], [RFC1035], [RFC2782] and [RFC4033], and security-related terminology from [RFC4949] and [RFC5280]. The terms "source domain", "derived domain", "reference identifier", and "presented identifier" are used as defined in the "CertID" specification [RFC6125].

This document is applicable to connections made from an XMPP client to an XMPP server ("_xmpp-client._tcp") or between XMPP servers ("_xmpp-server._tcp"). In both cases, the XMPP initiating entity acts as a TLS client and the XMPP receiving entity acts as a TLS server. Therefore, to simplify discussion this document uses "_xmpp-client._tcp" to describe to both cases, unless otherwise indicated.

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 [RFC2119].

3. Requirements

An XMPP initiating entity (TLS client) that wishes to use this prooftype MUST do so before exchanging stanzas addressed to the source domain. In general, this means that the proof MUST be completed before the XMPP stream is restarted following STARTTLS negotiation (as specified in [RFC6120]). However, connections between XMPP servers MAY also use this prooftype to verify the addition of new source domains onto an existing connection, such as multiplexing or "piggybacking" via [XEP-0220].

4. Secure Delegation

An XMPP initiating entity (TLS client) that wishes to use this prooftype performs the following actions:

1. Query for the appropriate SRV resource record for the source domain (e.g. "_xmpp-client._tcp.im.example.com").

2. If there is no SRV resource record, pursue the fallback methods described in [RFC6120].

3. If there is an SRV resource record, validate that the SRV record answer is secure according to [RFC4033]. If the answer is insecure, then delegation to the derived domain(s), as indicated by the "target host" field, is insecure and the TLS client MUST treat only the source domain as a reference identifier during certificate verification, as described in [RFC6120]; if the answer is bogus, the TLS client MUST abort.

4. If the answer is secure, the TLS client SHOULD consider any derived domain(s) in the answer as securely delegated; during certificate verification, the TLS client MUST treat both the source domain and the derived domain to which it has connected as reference identifiers.

5. Prooftype

[DANE] provides additional tools to verify the keys used in TLS

connections. A TLS client MAY use [DANE] for TLS certificate verification; its use depends on the delegation status of the source domain, as described in the following sections.

5.1. No Service Records

If no SRV records are found for the source domain, then the TLS client MUST query for a TLSA resource record as described in [DANE], where the prepared domain name MUST contain the source domain and the IANA-registered port 5222 for client-to-server streams (e.g. "_5222._tcp.im.example.com") or the IANA-registered port 5269 for server-to-server streams (e.g. "_5269._tcp.im.example.com").

In this case, the TLS client MUST treat only the source domain as its reference identifier during certificate verification, as described in [RFC6120].

5.2. Insecure Delegation

If the delegation of a source domain to a derived domain is not secure, then the TLS client MUST NOT make a TLSA record query to the derived domain as described in [DANE]. Instead, the TLS client MUST treat only the source domain as its reference identifier during certificate verification, as described in [RFC6120], and MUST NOT use [DANE].

5.3. Secure Delegation

If the source domain has been delegated to a derived domain in a secure manner as described under Section 4, then the TLS client MUST query for a TLSA resource record as described in [DANE], where the prepared domain name MUST contain the derived domain and a port obtained from the SRV answer (e.g., "_5555._tcp/hosting.example.net" for an SRV record such as "_xmpp-client._tcp.im.example.com IN TLSA 1 1 5555 hosting.example.net").

If no TLSA resource records exist for the specified service, then the TLS client MUST perform certificate verification as described under Section 4.

If TLSA resource records exist for the specified service, then the TLS client MUST treat the derived domain(s) as its reference identifier during certificate verification, using the information from the TLSA answer as the basis for verification as described in [DANE].

6. Internationalization Considerations

If the SRV, A/AAAA, and TLSA record queries are for an internationalized domain name, then they need to use the A-label form as defined in [RFC5890].

7. Security Considerations

This document supplements but does not supersede the security considerations provided in [RFC4033], [RFC6120], [RFC6125], and [DANE].

8. IANA Considerations

This document has no actions for the IANA.

9. Normative References

[DANE] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", draft-ietf-dane-protocol-23 (work in progress), June 2012.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

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

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, August 2010.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, March 2011.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, March 2011.

[XEP-0220] Miller, J., Saint-Andre, P., and P. Hancke, "Server Dialback", XSF XEP 0220, August 2011.

[XMPP-DNA] Saint-Andre, P. and M. Miller, "Domain Name Associations (DNA) in the Extensible Messaging and Presence Protocol (XMPP)", draft-saintandre-xmpp-dna-00 (work in progress), June 2012.

Authors' Addresses

Matthew Miller
Cisco Systems, Inc.
1899 Wynkoop Street, Suite 600
Denver, CO 80202
USA

Email: mamille2@cisco.com

Peter Saint-Andre
Cisco Systems, Inc.
1899 Wynkoop Street, Suite 600
Denver, CO 80202
USA

Email: psaintan@cisco.com