Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 13, 2012

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

June 6, 2012

Using DNSSEC and DANE as a Prooftype for XMPP Delegation
draft-miller-xmpp-dnssec-prooftype-00

Abstract

This document defines a model for securely delegating an XMPP service for a domain to a host associated with a different domain.

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 13, 2012.

Table of Contents

1. Introduction

In the core XMPP specification [RFC6120], the domain to which an XMPP initiating entity wants to connect is asserted via the 'to' attribute of the <stream:stream> header, and the TLS certificate offered by the receiving server is required to match this source domain (e.g., "im.example.com"). However, this model can cause problems if the source domain is delegated (via DNS SRV records [RFC2782]) to a host associated with a different domain that is derived via SRV (e.g., "hosting.example.net"), since the derived domain might also be the delegate for a number of other source domains and, for operational and security reasons, a hosting server is rarely able to present a certificate that matches the source domain.

Absent the use of DNS Security [RFC4033], delegation via SRV does not provide a strong basis for checking the derived domain rather than the source domain. This document describes how the use of DNSSEC with SRV results in more secure delegation, such that the initiating XMPP server can legitimately check the derived domain rather than the source domain.

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" and "derived domain" 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 the prooftype 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 delegations of additional source domains onto an existing connection, such as multiplexing via [XEP-0220].

4. Use of DNSSEC

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 or bogus, then delegation to the derived domain (as indicated by the "target host" field) is insecure and the TLS client MUST verify the certificate against the source domain as described in [RFC6120].

4. If there is an SRV record, for each derived domain from the SRV record answer (e.g. "hosting.example.net"), query for the "A" and/or "AAAA" resource records as described in [RFC6120].

5. For each derived domain, validate that the address record answers are provably secure according to [RFC4033]

6. If any answer is insecure or bogus, then the TLS client MUST NOT consider a connection to that derived domain as securely delegated from the source domain; when verifying the certificate, the TLS client MUST do so against the source domain as described in [RFC6120].

7. For each address record answer that is a provably secure, the TLS client SHOULD consider a connection to that derived domain as securely delegated; when verifying the certificate (as described in [RFC6125]), the TLS client SHOULD do so against the derived domain but MAY also verify the certificate against the source domain.

5. Use of DANE

[DANE] provides additional tools to verify the keys used in TLS connections. Whether it is appropriate to use [DANE] for TLS certificate verification depends on the delegation status of the source domain, as described in the following sections.

5.1. No Delegation

If the source domain has not been delegated to a derived domain, i.e., if the source domain and the derived domain are identical (e.g., "im.example.com"), then the TLS client MAY query for a TLSA resource record as described in [DANE], where the prepared domain name MUST contain the source domain and a port of 5222 for client-to-server streams (e.g. "_5222._tcp.im.example.com") or 5269 for server-to-server streams (e.g. "_5269._tcp.im.example.com").

In this case, the TLS client MUST perform certificate verification against the source domain 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 perform certificate verification against the source domain as described in [RFC6120], and MAY make a TLSA query against the source domain.

5.3. Secure Delegation

If the source domain has been delegated to a derived domain in a secure manner as described under [protocol], then the TLS client SHOULD query for a TLSA resource record as described in [DANE], where the prepared domain name MUST contain the derived domain and a port of 5222 for client-to-server streams or 5269 for server-to-server streams (e.g. "_5222._tcp.hosting.example.net").

If no TLSA resource records exist for the specified service, then the TLA client MUST perform certificate verification against the source domain as described in [RFC6120].

If TLSA resource records exist for the specified service, then the TLS client MUST perform certificate verification against the derived domain, using the information from the TLSA answer as the basis for verification as described in [DANE].

5.4. TLSA Certificate Usage 3 Considerations

If a TLSA resource record specifies certificate usage 3 (also known as "domain-issued certificate"), verification MUST NOT consider the source or derived domain. Instead, the target certificate MUST match the TLSA record, as specified in [DANE]. If matched, the TLS connection MUST considered valid for the source domain regardless of the target certificate's information.

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. References

[DANE] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", Internet-Draft draft-ietf-dane-protocol-21, May 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.

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