Network Working Group	J. Hildebrand
Internet-Draft	Cisco Systems, Inc.
Intended status: Standards Track	March 08, 2011
Expires: September 09, 2011	

DNSSEC for XMPP SRV Records

draft-hildebrand-xmpp-dnssec-00.txt

Abstract

This document proposes that DNS SRV records that can be trusted via DNSSEC signatures may be used to generate a list of acceptable names to check on server certificates offered by TLS.

Status of this Memo

Copyright Notice

Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction

XMPP uses SRV records for clients and servers to find servers for a given domain. Today, since the SRV record cannot be trusted, the server has to offer a TLS certificate that matches the original domain name, rather than one for the hostname in the SRV record. Deployment of delegated hosts would be much easier if the host could offer a certificate with the host name, rather than having to offer a certificate with the original domain name.

This document proposes that the server may offer a cert with any of the names generated from looking up trusted DNS entries.

Note: this document is only intended as a placeholder; it will be dramatically expanded later. As well it is likely that this approach is useful for protocols other than XMPP.

2. Conventions Used In This Document

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. Overview

The following steps are followed by a provider hosting "example.com" on the server "host1.example.net":

1. The owner of "example.com" serves an SRV record for "_xmpp-server._tcp.example.com" and "_xmpp-client._tcp.example.com", for example "0 1 5269 host1.example.net." might be used for each.

2. The owner of "example.com" MUST ensure that "example.com" is signed using DNSSEC [RFC4035], and that the SRV record is also signed using DNSSEC.

3. The hosting provider at "host1.example.net" generates a [RFC5280] PKIX certificate and has it signed by a widely-trusted Certificate Authority.

4. The hosting provider offers the generated certificate to anyone who connects and wants to talk to "example.com".

The following steps are followed by an initiating entity connecting to "example.com":

1. The initiator starts with an empty name list L.

2. The initiator adds the original domain name ("example.com" here) to L

3. The initiator does the normal SRV lookup, asking its resolver for DNSEC trust information.

4. For each hostname, CNAME, A or AAAA record that the initiator finds which is fully trustable according to DNSSEC, that name or IP address is added to L.

5. The initiator connects to the server as specified in XMPP [I-D.ietf-xmpp-3920bis], specifying "example.com" in the stream to attribute. Other protocols might use SNI [RFC4366] to indicate the desired host name.

6. The initiator MUST check each name in L against the certificate offered by the responder, using the rules specified in section 13.7.2 of [I-D.ietf-xmpp-3920bis] (or the equivalent rules for the target protocol).

4. Dialback considerations

TODO: how to share connections
TODO: interactions with dialback piggybacking

5. IANA Considerations

[TODO]

6. Security Considerations

Much more to follow here.

7. References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC4035]	Arends, R., Austein, R., Larson, M., Massey, D. and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.
[RFC4366]	Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J. and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, April 2006.
[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.
[I-D.ietf-xmpp-3920bis]	Saint-Andre, P, "Extensible Messaging and Presence Protocol (XMPP): Core", Internet-Draft draft-ietf-xmpp-3920bis-22, December 2010.

Appendix A. Acknowledgments

[TODO]

Author's Address

Joe Hildebrand Hildebrand Cisco Systems, Inc. 1899 Wyknoop Street, Suite 600 Denver, CO 80202 USA EMail: jhildebr@cisco.com