DANE
Internet-Draft
Intended status: Informational
Expires: April 30, 2015

D. York
Internet Society

October 27, 2014

DANE Deployment Observations
draft-york-dane-deployment-observations-00

Abstract

This document provides some observations about the deployment of the DANE protocol to date and some questions for discussion on the DANE mailing list and potentially at the IETF 91 meeting of the DANE Working Group.

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 April 30, 2015.

Table of Contents

1. Introduction

The DANE protocol defined in RFC 6698 provides a mechanism for specifying in DNS the Transport Layer Security (TLS) certificate or trust anchor (ex. certificate authority) to be used for a given domain. As the DANE protocol is being more widely deployed, we can observe some of the challenges seen to date. This document attempts to capture some of those observations and poses some questions for further consideration. Feedback on this document is welcome.

2. Observations

As I have been helping people understand the value of using DANE I have observed the following points related to deploying DANE:

- AWARENESS OF DANE - I have found that most people are completely unaware that DANE exists. Once people are informed about DANE and how it works, they usually see the value.

- CREATION OF TLSA RECORDS - Some people have found it difficult to create the TLSA records. Newer tools such as hashslinger and Shumon Huque's website are helping make this easier, but more tools need to be available.

- INABILITY TO ENTER TLSA RECORDS AT DNS HOSTING OPERATORS - One of the biggest deployment challenges has turned out to be that many people are unable to enter TLSA records in the provisioning interface for their DNS hosting operator. Those interfaces are typically web-based and allow a user to add only a certain set of RRTYPES to a DNS zone file. Until the DNS hosting provider allows users to add a TLSA record, those users will not be able to publish TLSA records and use DANE.

- AVAILABILITY OF DEVELOPER LIBRARIES - Some people have found that DANE support is not yet included in the DNS library they have previously used. This is changing as DANE is added to more DNS libraries. The new getDNS API is also helpful to have.

- PERCEPTION THAT DANE IS ONLY FOR SELF-SIGNED CERTIFICATES - Some people who have heard of DANE believe that is only for people using self-signed certificates. They do not understand that it can also be used with certificates from an existing certificate authority (CA).

- PERFORMANCE - A few people have raised concerns about the additional DNS queries required to complete the DANE transaction and wondered about the performance impact.

- CRYPTOGRAPHIC CONCERNS - A few concerns have been raised that DANE is cryptographically weaker than other potential solutions, although in further discussion this often seems to be more of a perception issue and not fully understanding how DANE can be used.

There are also questions about the availability of DNSSEC, but as that deployment is increasing on both the signing and validation side and tools are now more readily available, I've chosen here to focus more on observations I have heard directly related to DANE.

3. Questions

Several potential questions for discussion include:

- What roadblocks are people running into with implementing DANE? (outside of the broader issue of getting DNSSEC validation and signing more widely available) are there lessons we can feed back into our process of developing DANE-related standards?

- Are there more "Using DANE with <foo>" types of documents that we can or should create? (and who is willing to do so?)

- Are there some good examples/case studies of DANE implementations that we could perhaps capture as informational RFCs? (the Jabber community's implementation comes to mind)

- Are there places where it would be helpful if there were reference implementations of DANE support? For example, DANE for email got a boost when support was added to postfix. Are there other commonly-used open source projects where the addition of DANE support would help move deployment along?

- Are there test tools that need to be developed? or existing ones that need to be better promoted? are there interop tests we can arrange?

4. IANA Considerations

This document requests no actions from the IANA.

5. Security Considerations

This document raises no specific security considerations.

6. References

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

Appendix A. Acknowledgements

(to be added)

Author's Address

Dan York
Internet Society

Email: york@isoc.org
URI: https://www.internetsociety.org/