Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: July 11, 2016

S. Huque
Verisign Labs
V. Dukhovni
Two Sigma

January 08, 2016

TLS Extension for DANE Client Identity
draft-huque-tls-dane-clientid-00

Abstract

This document specifies a TLS and DTLS extension to convey a DNS-Based Authentication of Named Entities (DANE) Client Identity to a TLS or DTLS server. This is useful for applications that perform TLS client authentication via DANE TLSA records.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document specifies a Transport Layer Security (TLS) extension [RFC6066] to convey a DANE [RFC6698] Client Identity to the TLS server. This is useful for applications that perform TLS client authentication via DANE TLSA records, as described in [DANECLIENT]. The conveyed identity is in the form of a domain name associated with the client that is expected to have a corresponding DANE TLSA record published in the DNS.

This extension supports both TLS and DTLS [RFC6347], and the term TLS in this document is used generically to describe both protocols.

2. Overview

When TLS clients use X.509 client certificates or raw public keys that are authenticated via DANE TLSA records, they need a mechanism to convey their DANE identity to the server. The TLS extension defined in this document is used to accomplish this. Upon receipt of this extension, a TLS server learns the client's identity and the fact that the client expects that the server can authenticate it via a corresponding DNSSEC-validated TLSA record.

In the case of X.509 client certificates, a TLS server can learn the client's identity by examining subject alternative names included in the certificate itself. However, without a mechanism such as the one defined in this extension, the TLS server cannot know apriori that the client has a published TLSA record, and thus may unnecessarily issue DNS queries for DANE TLSA records in-band with the TLS handshake even in cases where the client has no TLSA record associated with it. When multiple identities are present in the certificate, a client can use this extension to specify exactly which one the server should use. An additional situation in which this extension helps is where some TLS servers may need to selectively prompt for client certificate credentials only for clients that are equipped to provide certificates.

When TLS raw public keys [RFC7250] are being used to authenticate the client, the client uses this extension to explicitly indicate to the server what its domain name identity is.

Detailed protocol behavior of TLS clients and servers is described in [DANECLIENT].

3. DANE Client Identity Extension

The DANE Client Identity Extension type, "dane_clientid", will have a value assigned and registered in the IANA TLS Extensions registry.

A TLS client implementing this specification SHOULD send an extension of type "dane_clientid" in the ClientHello handshake message to TLS servers it intends to perform DANE client authentication with.

The "extension_data" field of the extension MUST contain a "DaneClientName" data structure defined in the following format:

```
   enum {
       dns_name(0), srv_name(1), (255)
   } NameType;

   opaque dNSName<1..2^16-1>;
   opaque SRVName<1..2^16-1>;

   struct {
       NameType name_type;
       select (name_type) {
           case dns_name: dNSName;
           case srv_name: SRVName;
       } name;
   } DaneClientName;
```

The opaque dNSName or SRVName field contains the domain name of the client in textual presentation format, as described in RFC 1035 [RFC1035].

4. Open Questions

Should multiple client names be supported in the extension?

Is the dNSName/SRVName distinction useful, or can we just simplify and use only dNSName? These two name forms are analogous to the two recommended for use in X.509 certificates in the DANE client authentication draft, so the server could use this to additionally check against the corresponding certificate fields (but does it need to?). If the server needs a hint of whether to construct an application specific ID, then this might be useful, but this could also be inferred from the structure of the name and the client could just specify an application specific identity in the dNSName type.

The extension is defined in terms of a DANE specific identity. Is there a need for a more general purpose client name indication extension? If so, this extension could be renamed and augmented to have an additional usage field containing values denoting DANE or alternative application usages.

5. Security Considerations

To prevent unnecessary privacy leakage of the client's name in cleartext, a TLS client implementing this specification should be configured to only send this extension to TLS servers it intends to perform client authentication with.

6. IANA Considerations

This extension requires the registration of a new value in the TLS ExtensionsType registry. If the draft is adopted by the WG, the authors expect to make an early allocation request as specified in [RFC7120]

7. References

7.1. Normative References

[DANECLIENT]
Huque, S., James, D., and V. Dukhovni, "TLS Client Authentication via DANE TLSA Records", , <https://tools.ietf.org/html/draft-huque-dane-client-cert>.

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

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC6066] Eastlake, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

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

[RFC7250] Wouters, P., Tschofenig, H., Gilmore, J., Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7250, June 2014.

7.2. Informative References

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

Authors' Addresses

Shumon Huque
Verisign Labs

Email: shuque@verisign.com

Viktor Dukhovni
Two Sigma

Email: ietf-dane@dukhovni.org