TLS
Internet-Draft
Intended status: Standards Track
Expires: September 28, 2019

M. Thomson
Mozilla

March 27, 2019

Suppressing Intermediate Certificates in TLS
draft-thomson-tls-sic-00

Abstract

A TLS client that has access to the complete set of published intermediate certificates can inform servers of this fact so that the server can avoid sending intermediates, reducing the size of the TLS handshake.

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 https://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 September 28, 2019.

Table of Contents

1. Introduction

In some uses of public key infrastructure (PKI) intermediate certificates are used to sign end-entity certificates. In the web PKI, clients require that certificate authorities disclose all intermediate certificates that they create. Though the set of intermediate certificates is large, the size is bounded, so it is possible to provide a complete set of certificates.

For a client that has all intermediates, having the server send intermediates in the TLS handshake increases the size of the handshake unnecessarily. This document creates a signal that a client can send that informs the server that it has a complete set of intermediates. A server that receives this signal can limit the certificate chain it sends to just the end-entity certificate, saving on handshake size.

This mechanism is intended to be complementary with certificate compression [COMPRESS] in that it reduces the size of the handshake.

2. Terms and Definitions

The keywords "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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Got Intermediates Flag

A client that believes that it has a current, complete set of intermediate certificates sends the tls_flags extension [TLS-FLAGS] with the 0xTBD flag set to 1. A server can also set the flag in a CertificateRequest extension.

A server that receives a value of 1 in the 0xTBD flag from a ClientHello message SHOULD omit all certificates other than the end-entity certificate from its Certificate message. A client that receives a value of 1 in the 0xTBD flag in a CertificateRequest message SHOULD omit all certificates other than the end-entity certificate from the Certificate message that it sends in response.

The 0xTBD flag can only be send in a ClientHello or CertificateRequest message. Endpoints that receive a value of 1 in any other handshake message MUST generate a fatal illegal_parameter alert.

4. Security Considerations

This creates an unencrypted signal that might be used to identify which clients believe that they have all intermediates. This might allow cilents to be more effectively fingerprinted by peers and any elements on the network path.

5. IANA Considerations

This document registers the 0xTBD flag in the registry created by [TLS-FLAGS].

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[TLS-FLAGS] Nir, Y., "A Flags Extension for TLS 1.3", draft-nir-tls-tlsflags-00 (work in progress), March 2019.

6.2. Informative References

[COMPRESS] Ghedini, A. and V. Vasiliev, "TLS Certificate Compression", draft-ietf-tls-certificate-compression-04 (work in progress), October 2018.

Author's Address

Martin Thomson
Mozilla

Email: mt@lowentropy.net