HTTPbis Working Group
Internet-Draft
Intended status: Informational
Expires: September 25, 2015

M. Bishop
Microsoft

March 24, 2015

TLS Renegotiation Support Extension to HTTP/2
draft-bishop-support-reneg-00

Abstract

The HTTP/2 spec requires that TLS renegotiation not be employed when the negotiated application protocol is HTTP/2. This document defines an extension to HTTP/2 which permits renegotiation to be employed by peers which mutually consent to do so, while allowing peers to understand whether renegotiation is permitted before attempting it.

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 September 25, 2015.

Table of Contents

1. Introduction

The HTTP/2 spec [I-D.ietf-httpbis-http2] restricts TLS renegotiation to before the transmission of the HTTP/2 connection preface. TLS renegotiation is broadly employed to permit the use of client certificates as an authentication mechanism. The use of client certificates is required by law in certain jurisdictions and required to support upgrading existing applications to HTTP/2 transparently. Although other mechanisms have been proposed ([I-D.thomson-tls-care], [I-D.thomson-httpbis-catch], [I-D.nottingham-http-over-version], the HTTP_1_1_REQUIRED error code in [I-D.ietf-httpbis-http2]), these uniformly require a separate TCP connection. On this separate TCP connection, the client would employ either a changed TLS semantic that must be understood by both sides, or renegotiation underneath an application protocol which does not prohibit it.

This document defines an extension which permits mutually-consenting HTTP/2 implementations to perform renegotiation on the existing HTTP connection when the security properties of renegotiation are acceptable for their scenarios and the TLS version in use supports it.

1.1. Conventions and Terminology

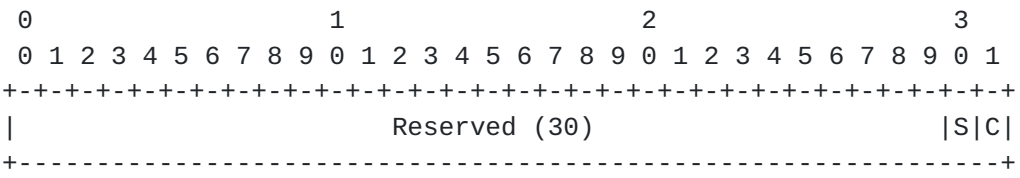
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

All numeric values are in network byte order. Values are unsigned unless otherwise indicated. Literal values are provided in decimal or hexadecimal as appropriate. Hexadecimal literals are prefixed with "0x" to distinguish them from decimal literals.

2. The TLS_RENEG_PERMITTED Setting

This document defines a new setting value in HTTP/2, TLS_RENEG_PERMITTED, with code TBD and an initial value of 0x00.

The thirty-two bits of the setting value are interpreted as follows:



Setting Value Definition

The effective state for an HTTP/2 connection is the bitwise AND of the values sent by each peer.

Either peer is permitted to initiate TLS renegotiation if this behavior is mutually agreeable. The recipient MUST treat a TLS renegotiation as a connection error of type PROTOCOL_ERROR if support for renegotiation has not previously been agreed upon.

The defined bits are:

C (Bit 0) If set, client-initiated renegotiation is allowed.

S (Bit 1) If set, server-initiated renegotiation is allowed.

All other bits are undefined, and MUST be zero when sent and ignored upon receipt.

3. Security Considerations

In [RFC5746], an attack is described in which renegotiation can be exploited by an intermediary to inject attacker-controlled content before the content contained in the TLS connection the client believes it has established with the server. The TLS extension described in that document cryptographically ties the sessions and prevents the attack described.

HTTP/2 includes attributes which would make a similar attack more challenging than in HTTP/1.1. Thus, renegotiation in HTTP/2 may be preferable to renegotiation under an HTTP/1.1 connection. Implementers will need to consider the security context of the current connection when deciding when to offer this extension.

4. IANA Considerations

A new setting is defined for HTTP/2 in the "HTTP/2 Settings" registry.

- Name: TLS_RENEG_PERMITTED
- Code: TBD
- Initial value: 0x00
- Specification: This document

5. References

5.1. Normative References

[I-D.ietf-httpbis-http2]
Belshe, M., Peon, R., and M. Thomson, "Hypertext Transfer Protocol version 2", draft-ietf-httpbis-http2-17 (work in progress), February 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

5.2. Informative References

[I-D.nottingham-http-over-version]
Nottingham, M., "The Over-Version HTTP Response Header Field", draft-nottingham-http-over-version-00 (work in progress), June 2014.

[I-D.thomson-httpbis-catch]
Thomson, M., "Client Authentication over TLS Connection Header", draft-thomson-httpbis-catch-00 (work in progress), March 2014.

[I-D.thomson-tls-care]
Thomson, M., "Client Authentication Request Extension for (D)TLS", draft-thomson-tls-care-00 (work in progress), March 2014.

[RFC5746] Rescorla, E., Ray, M., Dispensa, S., and N. Oskov, "Transport Layer Security (TLS) Renegotiation Indication Extension", RFC 5746, February 2010.

Author's Address

Mike Bishop
Microsoft

EMail: michbish@microsoft.com