HTTP
Internet-Draft
Updates: 7540 (if approved)
Intended status: Standards Track
Expires: March 23, 2020

D. Benjamin
Google LLC

September 20, 2019

Using TLS 1.3 with HTTP/2
draft-ietf-httpbis-http2-tls13-02

Abstract

This document updates HTTP/2 to prohibit TLS 1.3 post-handshake authentication, as an analog to existing TLS 1.2 renegotiation restriction.

Note to Readers

RFC EDITOR: please remove this section before publication

Discussion of this draft takes place on the HTTP working group mailing list (ietf-http-wg@w3.org), which is archived at https://lists.w3.org/Archives/Public/ietf-http-wg/ [1].

Working Group information can be found at https://httpwg.org/ [2]; source code and issues list for this draft can be found at https://github.com/httpwg/http-extensions/labels/http2-tls13 [3].

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 March 23, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Requirements Language 3
3. Post-Handshake Authentication in HTTP/2 3
4. Other Post-Handshake TLS Messages in HTTP/2 3
5. Security Considerations 4
6. IANA Considerations 4
7. References 4
7.1. Normative References 4
7.2. Informative References 5
7.3. URIs 5
Author's Address 5

1. Introduction

TLS 1.2 [RFC5246] and earlier support renegotiation, a mechanism for changing parameters and keys partway through a connection. This was sometimes used to implement reactive client authentication in HTTP/1.1 [RFC7230], where the server decides whether to request a client certificate based on the HTTP request.

HTTP/2 [RFC7540] multiplexes multiple HTTP requests over a single connection, which is incompatible with the mechanism above. Clients cannot correlate the certificate request with the HTTP request which triggered it. Thus, Section 9.2.1 of [RFC7540] forbids renegotiation.

TLS 1.3 [RFC8446] updates TLS 1.2 to remove renegotiation in favor of separate post-handshake authentication and key update mechanisms. The former shares the same problems with multiplexed protocols, but the prohibition in HTTP/2 only applies to TLS 1.2 renegotiation.

This document updates HTTP/2 to similarly forbid TLS 1.3 post-handshake authentication.

2. Requirements Language

The key words "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. Post-Handshake Authentication in HTTP/2

HTTP/2 servers MUST NOT send post-handshake TLS 1.3 CertificateRequest messages. HTTP/2 clients MUST treat TLS 1.3 post-handshake authentication as a connection error (see Section 5.4.1 of [RFC7540]) of type PROTOCOL_ERROR.

[RFC7540] permitted renegotiation before the HTTP/2 connection preface to provide confidentiality of the client certificate. TLS 1.3 encrypts the client certificate in the initial handshake, so this is no longer necessary. HTTP/2 servers MUST NOT send post-handshake TLS 1.3 CertificateRequest messages before the connection preface.

The above applies even if the client offered the "post_handshake_auth" TLS extension. This extension is advertised independently of the selected ALPN protocol [RFC7301], so it is not sufficient to resolve the conflict with HTTP/2. HTTP/2 clients that also offer other ALPN protocols, notably HTTP/1.1, in a TLS ClientHello MAY include the "post_handshake_auth" extension to support those other protocols. This does not indicate support in HTTP/2.

4. Other Post-Handshake TLS Messages in HTTP/2

[RFC8446] defines two other messages that are exchanged after the handshake is complete, KeyUpdate and NewSessionTicket.

KeyUpdate messages only affect TLS itself and do not require any interaction with the application protocol. HTTP/2 implementations MUST support key updates when TLS 1.3 is negotiated.

NewSessionTicket messages are also permitted. Though these interact with HTTP when early data is enabled, these interactions are defined in [RFC8470] and allowed for in the design of HTTP/2.

Unless the use of a new type of TLS message depends on an interaction with the application layer protocol, that TLS message can be sent after the handshake completes.

5. Security Considerations

This document resolves a compatibility concern between HTTP/2 and TLS 1.3 when supporting post-handshake authentication with HTTP/1.1. This lowers the barrier for deploying TLS 1.3, a major security improvement over TLS 1.2.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. 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>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <https://www.rfc-editor.org/info/rfc7230>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/info/rfc7301>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <https://www.rfc-editor.org/info/rfc7540>.

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

7.2. Informative References

[RFC8470] Thomson, M., Nottingham, M., and W. Tarreau, "Using Early Data in HTTP", RFC 8470, DOI 10.17487/RFC8470, September 2018, <https://www.rfc-editor.org/info/rfc8470>.

7.3. URIs

[1] https://lists.w3.org/Archives/Public/ietf-http-wg/

[2] https://httpwg.org/

[3] https://github.com/httpwg/http-extensions/labels/http2-tls13

Author's Address

David Benjamin
Google LLC

Email: davidben@google.com