Workgroup: HTTP Working Group
Internet-Draft: draft-vvv-httpbis-alps
Published: 21 January 2021
Intended Status: Standards Track
Expires: 25 July 2021
Authors: V. Vasiliev
Google

Using TLS Application-Layer Protocol Settings (ALPS) in HTTP

Abstract

This document describes the use of TLS Application-Level Protocol Settings (ALPS) in HTTP/2 and HTTP/3. Additionally, it defines a set of additional HTTP SETTINGS parameters that would normally be impractical without ALPS.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the HTTPBIS Working Group mailing list (httpbis@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/httpbis/.

Source for this draft and an issue tracker can be found at https://github.com/vasilvv/httpbis-alps.

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 25 July 2021.

Copyright Notice

Table of Contents

1. Introduction

HTTP/2 defines a mechanism for exchanging the protocol settings using a SETTINGS frame ([RFC7540], Section 6.5). HTTP/3 uses a similar mechanism ([HTTP3], Section 7.2.4). One of the properties of the mechanism as defined by both of those protocols is that the parties start out without having access to the entirety of the peer's settings. This means that they have to initially operate using the default settings, and after receiving the SETTINGS frame, they have to find a way to transition from the default to the exchanged settings.

HTTP is commonly used in conjunction with TLS. TLS performs its own handshake that precedes any data being exchanged by the HTTP layer itself. The TLS Application-Level Protocol Settings extension [ALPS] allows settings negotiation to be performed within the TLS handshake, thus making the result immediately available to the HTTP layer as soon as the handshake completes. This removes the need for synchronizing settings, and makes them available earlier than they would be otherwise.

This document defines how ALPS is used with HTTP/2 and HTTP/3, and introduces certain new settings that would not be practical without ALPS.

2. Conventions and Definitions

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. Use of ALPS in HTTP

If ALPS is successfully negotiated during the TLS handshake for an HTTP/2 connection, the ALPS payload for both peers SHALL be a sequence of HTTP/2 frames. Frames SHALL NOT be present in ALPS unless they are explicitly allowed to be there; this document only allows the SETTINGS frame ([RFC7540], Section 6.5.1). Sending a SETTINGS frame in ALPS supersedes the requirement to send a SETTINGS frame at the beginning of the connection. All settings exchanged via ALPS SHALL be automatically treated as acknowledged.

If ALPS is successfully negotiated during TLS handshake for an HTTP/3 connection, the ALPS payload for both peers SHALL be a sequence of HTTP/3 frames. Frames SHALL NOT be present in ALPS unless they are explicitly allowed to be there; this document only allows the SETTINGS frame ([HTTP3], Section 7.2.4). Sending a SETTINGS frame in ALPS supersedes the requirement to send a SETTINGS frame at the beginning of the control stream.

Since settings exchanged through ALPS are always available at the beginning of the connection, some HTTP extensions may opt to require those to be sent through ALPS. Such extensions are exempt from the initialization requirements of the Section 7.2.4.2 of [HTTP3].

4. Security Considerations

In ALPS, both client and server settings are sent encrypted. Settings communicated through ALPS are presented to all clients before they are authenticated; thus, if a server relies on TLS client authentication and considers its settings private, it MUST NOT use the mechanism defined in this document.

5. IANA Considerations

IANA will add an "Allowed in ALPS" column to the "HTTP/2 Frames" section of the "Hypertext Transfer Protocol version 2 (HTTP/2) Parameters" registry, with a value set to "Yes" for SETTINGS (0x4), and to "No" for all other previously defined settings.

TODO: Add HTTP/3 once IANA has an HTTP/3 registry.

6. Normative References

[ALPS] Vasiliev, V., "TLS Application-Layer Protocol Settings Extension", Work in Progress, Internet-Draft, draft-vvv-

tls-alps-latest, <https://tools.ietf.org/html/draft-vvv-tls-alps-latest>.

[HTTP3] Bishop, M., Ed., "Hypertext Transfer Protocol Version 3 (HTTP/3)", Work in Progress, Internet-Draft, draft-ietf-quic-http-latest, <https://tools.ietf.org/html/draft-ietf-quic-http-latest>.

[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>.

[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>.

Acknowledgments

This document has benefited from contributions and suggestions from David Benjamin, Nick Harper, David Schinazi, and many others.

Author's Address

Victor Vasiliev
Google

Email: vasilvv@google.com