Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 07, 2013

S.F. Friedl
Cisco Systems, Inc.
A.P. Popov
Microsoft Corp.

April 05, 2013

Transport Layer Security (TLS) Application Layer Protocol Negotiation Extension
draft-ietf-tls-applayerprotoneg-00

Abstract

This document describes a Transport Layer Security (TLS) extension for application layer protocol negotiation within the TLS handshake. For instances in which the TLS connection is established over a well known TCP/IP port not associated with the desired application layer protocol, this extension allows the application layer to negotiate which protocol will be used within the TLS session.

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 October 07, 2013.

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. Application Layer Protocol Negotiation 3
3.1. The Application Layer Protocol Negotiation Extension . . 3
3.2. Protocol Selection 5
4. Design Considerations 6
5. Security Considerations 6
6. IANA Considerations 7
7. Acknowledgements 7
8. References 7
8.1. Normative References 7
8.2. Informative References 8
Authors' Addresses 8

1. Introduction

Currently, the Next Protocol Negotiation extension (NPN) is used to establish a SPDY [spdy] protocol session within a TLS RFC 5246 [RFC5246] session on port 443. NPN is not specific to SPDY and can be used to negotiate sessions for a wide variety of protocols within the TLS handshake.

NPN seeks to provide a reliable mechanism for application developers to establish secure sessions for arbitrary protocols without interference from firewalls, HTTP proxies and MITM proxies. It addresses this goal by introducing a protocol negotiation process into the TLS handshake under the constraints that no additional roundtrips be added to the handshake and that the final protocol selection be opaque to the network carrying the TLS session. Within the NPN extension, it is the server that first generates and transmits an offer of supported protocols to the client. The offer is sent as part of the TLS ServerHello message before the [ChangeCipherSpec] subprotocol has been started, therefore the list of protocols supported by the server is transmitted in plaintext. The client chooses a protocol which may or may not appear in the offer from the server and then responds with the definitive protocol selection answer. The client response is sent after the

[ChangeCipherSpec] subprotocol has been initiated, so the protocol selected is encrypted in the client response.

In many other application layer protocol negotiation processes, it is the client that first sends an offer of protocols it supports to the

server. The server then selects the protocol to be used in the session and includes this answer in the response. RFC 3264 [RFC3264] describes a SDP based offer/answer model which is not proscriptive in terms of which party generates the offer, however in practice it is typically the client generating the offer and the server replying with the answer. This permits the server to act as the definitive entity for selection of the application layer protocol.

This draft proposes an alternative formulation of the NPN protocol which 1) brings the offer/answer negotiation into alignment with the majority of other application layer protocol negotiation standards, 2) allows certificate selection based on the application protocol and 3) makes the definitive protocol selection answer from the server visible to the network, when the parties so desire.

2. Requirements Language

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].

3. Application Layer Protocol Negotiation

3.1. The Application Layer Protocol Negotiation Extension

A new extension type ("application_layer_protocol_negotiation(16)") is defined and MAY be included by the client in its "ClientHello" message.

```
enum {
    application_layer_protocol_negotiation(16), (65535)
} ExtensionType;
```

The "extension_data" field of the ("application_layer_protocol_negotiation(16)") extension SHALL

contain a "ProtocolNameList" value.

```
opaque ProtocolName<1..2^8-1>;

struct {
    ProtocolName protocol_name_list<2..2^16-1>
} ProtocolNameList;
```

"ProtocolNameList" contains the list of protocols advertised by the client, in descending order of preference. Protocols are named by IANA registered, opaque, non-empty byte strings. Implementations

MUST ensure that an empty string is not included and that no byte strings are truncated.

Experimental protocol names, which are not registered by IANA, will start with the following sequence of bytes: 0x65, 0x78, 0x70 ("exp").

Servers that receive a client hello containing the "application_layer_protocol_negotiation" extension, MAY return a suitable protocol selection response to the client. The server will ignore any protocol name that it does not recognize. A new ServerHello extension type ("application_layer_protocol_negotiation(16)") MAY be returned to the client within the extended ServerHello message. The "extension_data" field of the ("application_layer_protocol_negotiation(16)") extension SHALL be structured the same as described above for the client "extension_data", except that the "ProtocolNameList" MUST contain exactly one "ProtocolName".

The additional content associated with this extension MUST be included in the hash calculations associated with the "Finished" messages.

Therefore, a full handshake with the "application_layer_protocol_negotiation" extension in the ClientHello and ServerHello messages has the following flow (contrast with section 7.3 of RFC 5246 [RFC5246]):

Client Server

```
ClientHello                       -------->       ServerHello
  (ALPN extension &                                 (ALPN extension &
   list of protocols)                                selected protocol)
                                                  Certificate*
                                                  ServerKeyExchange*
                                                  CertificateRequest*
                                  <--------       ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                          -------->
                                                  [ChangeCipherSpec]
                                  <--------       Finished
Application Data                  <------->       Application Data
```

Figure 1

An abbreviated handshake with the "application_layer_protocol_negotiation" extension has the following flow:

```
Client                                              Server

ClientHello                       -------->       ServerHello
  (ALPN extension &                                 (ALPN extension &
   list of protocols)                                selected protocol)
                                                  [ChangeCipherSpec]
                                  <--------       Finished
[ChangeCipherSpec]
Finished                          -------->
Application Data                  <------->       Application Data
```

Figure 2

Unlike many other TLS extensions, this extension does not establish properties of the session, only of the connection. When session resumption or session tickets RFC 5077 [RFC5077] are used, the previous contents of this extension are irrelevant and only the values in the new handshake messages are considered.

3.2. Protocol Selection

It is expected that a server will have a list of protocols that it supports, in preference order, and will only select a protocol if the client supports it. In that case, the server SHOULD select the most highly preferred protocol it supports which is also advertised by the client. In the event that the server supports no protocols that the client advertises, then the server SHALL respond with a fatal "no_application_protocol" alert.

```
enum {
    no_application_protocol(120),
    (255)
} AlertDescription;
```

The "no_application_protocol" fatal alert is only defined for the "application_layer_protocol_negotiation" extension and MUST NOT be sent unless the server has received a ClientHello message containing this extension.

The protocol identified in the "application_layer_protocol_negotiation" extension type in the ServerHello SHALL be definitive for the connection. The server SHALL NOT respond with a selected protocol and subsequently use a different protocol for application data exchange.

4. Design Considerations

The ALPN extension is intended to follow the typical design of TLS protocol extensions. Specifically, the negotiation is performed entirely within the client/server hello exchange in accordance with established TLS architecture. The "application_layer_protocol_negotiation" ServerHello extension is intended to be definitive for the connection and is sent in plaintext to permit network elements to provide differentiated service for the

connection when the TCP/IP port number is not definitive for the application layer protocol to be used in the connection. By placing ownership of protocol selection on the server, ALPN facilitates scenarios in which certificate selection or connection rerouting may be based on the negotiated protocol.

Finally, by managing protocol selection in the clear as part of the handshake, ALPN avoids introducing false confidence with respect to the the ability to hide the negotiated protocol in advance of establishing the connection. If hiding the protocol is required, then renegotiation after connection establishment, which would provide true TLS security guarantees, would be a preferred methodology.

A namespace will be assigned for experimental protocols, comprising byte strings which start with the following sequence of bytes: 0x65, 0x78, 0x70 ("exp"). Assignments in this namespace do not need IANA registration.

5. Security Considerations

The ALPN extension does not impact the security of TLS session establishment or application data exchange. ALPN serves to provide an externally visible marker for the application layer protocol associated with the TLS connection. Historically, the application layer protocol associated with a connection could be ascertained from the TCP/IP port number in use.

Encrypting the selected application protocol information and sending it before the Finished messages are exchanged, as done in NPN, does not provide confidentiality guarantees due to the possibility of man-in-the-middle attacks.

6. IANA Considerations

The IANA has updated its Registry of TLS ExtensionType Values to include the following entry:

- 16 application_layer_protocol_negotiation

This document also requires the IANA to create a registry of

Application Layer Protocol Negotiation protocol byte strings, initially containing the following entries:

- "http/1.1": HTTP/1.1 [RFC2616];

- "http/2.0": HTTP/2.0;

- "spdy/1": (obsolete) SPDY version 1;

- "spdy/2": SPDY version 2;

- "spdy/3": SPDY version 3.

We propose that this new registry be created in a new page entitled: "Application Layer Protocol Negotiation (ALPN) Protocol IDs" beneath the existing heading of "Transport Layer Security (TLS)".

7. Acknowledgements

This document benefitted specifically from the NPN extension draft authored by Adam Langley of Google and from discussions with Tom Wesselman and Cullen Jennings both of Cisco.

8. References

8.1. Normative References

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

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[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.

8.2. Informative References

[RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, January 2008.

[spdy] Belshe, M. and R. Peon, "SPDY Protocol (Internet Draft)", 2012.

Authors' Addresses

Stephan Friedl
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

Phone: (720)562-6785
Email: sfriedl@cisco.com

Andrei Popov
Microsoft Corp.
One Microsoft Way
Redmond, WA 98052
USA

Email: andreipo@microsoft.com