Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 25, 2017

N. Mavrogiannopoulos
Red Hat
D. Woodhouse
Intel

September 21, 2016

A TLS application-specific identifier
draft-mavrogiannopoulos-app-id-00

Abstract

This memo proposes an application-specific identifier for use with the TLS and DTLS protocols. It defines a TLS extension to allow an arbitrary identifier to be specified in the Client Hello, which can be used for application-specific routing purposes.

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 March 25, 2017.

1. Introduction

In certain applications, a TLS or DTLS session follows-up a previously established communication channel which has already assigned the user to a particular server from a pool or a particular system process. In these cases it is desirable for the follow-up sessions to be forwarded by a routing process or system to the initial handler, early, prior to any TLS negotiation.

That can be implemented with an application-specific identifier which will be included by the client on its initial Client Hello message. The routing processor will utilize that identifier to forward the session to the appropriate handler. This document describes a way for applications to attach application-specific identifiers to the Client Hello message.

2. Terminology

This document uses the same notation and terminology used in the TLS and DTLS protocol specifications [RFC5246][RFC6347].

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 [RFC2119].

3. TLS Extension: Application-specific identifier

The TLS application-specific identifier is an arbitrary byte sequence encoded in the Client Hello as an extension. It is applicable to both the TLS and DTLS protocols [RFC5246][RFC6347].

3.1. Extension Negotiation

In order to specify the identifier, clients include an extension of type "application_specific_identifier" to the extended client hello message. The "application_specific_identifier" TLS extension is assigned the value of TDB-BY-IANA from the TLS ExtensionType registry. This value is used as the extension number for the extensions in the client hello message. The server MUST NOT include a corresponding value to the Server Hello for this extension. The hello extension mechanism is described in [RFC5246].

This extension data have the following format.

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

The contents and size of ApplicationID are application-specific. Examples are, a 32-bit identifier, an 128-bit UUID [RFC4122], or a value defined by the application profile or policy.

4. Security Considerations

Applications and application profiles must ensure that they do not reveal sensitive data, or data that could compromise the TLS protocol's properties through the ApplicationID value.

5. IANA Considerations

This document defines a new TLS extension, "application_specific_identifier", assigned a value of TBD-BY-IANA (the value 48018 is suggested) from the TLS ExtensionType registry defined in [RFC5246]. This value is used as the extension number for the extensions in the client hello message.

6. References

6.1. Normative References

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

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <http://www.rfc-editor.org/info/rfc6347>.

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

6.2. Informative References

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <http://www.rfc-editor.org/info/rfc4122>.

Appendix A. Acknowledgements

Authors' Addresses

Nikos Mavrogiannopoulos
Red Hat, Inc.
Brno
Czech Republic

Email: nmav@redhat.com

David Woodhouse
Intel
UK

Email: dwmw2@infradead.org