

Internet Engineering Task Force (IETF)
Request for Comments: 9266
Updates: 5801, 5802, 5929, 7677
Category: Standards Track
ISSN: 2070-1721

S. Whited
July 2022

Channel Bindings for TLS 1.3

Abstract

This document defines a channel binding type, `tls-exporter`, that is compatible with TLS 1.3 in accordance with RFC 5056, "On the Use of Channel Bindings to Secure Channels". Furthermore, it updates the default channel binding to the new binding for versions of TLS greater than 1.2. This document updates RFCs 5801, 5802, 5929, and 7677.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <https://www.rfc-editor.org/info/rfc9266>.

Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction
 - 1.1. Conventions and Terminology
 2. The 'tls-exporter' Channel Binding Type
 3. TLS 1.3 with SCRAM or GSS-API over SASL
 4. Security Considerations
 - 4.1. Uniqueness of Channel Bindings
 - 4.2. Use with Legacy TLS
 5. IANA Considerations
 - 5.1. Registration of Channel Binding Type
 - 5.2. Registration of Channel Binding TLS Exporter Label
 6. References
 - 6.1. Normative References
 - 6.2. Informative References
- Author's Address

1. Introduction

The "tls-unique" channel binding type defined in [RFC5929] was found

to be susceptible to the "triple handshake vulnerability" [TRIPLE-HANDSHAKE] without the extended master secret extension defined in [RFC7627]. While TLS 1.3 uses a complete transcript hash akin to the extended master secret procedures, the safety of channel bindings with TLS 1.3 was not analyzed as part of the core protocol work, so the specification of channel bindings for TLS 1.3 was deferred. Appendix C.5 of [RFC8446] notes the lack of channel bindings for TLS 1.3; this document defines such channel bindings and fills that gap. Furthermore, this document updates [RFC5929] by adding an additional unique channel binding type, "tls-exporter", that replaces some usage of "tls-unique".

1.1. Conventions and Terminology

Throughout this document, the acronym "EKM" is used to refer to "Exported Keying Material" as defined in [RFC5705].

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.

2. The 'tls-exporter' Channel Binding Type

Channel binding mechanisms are not useful until TLS implementations expose the required data. To facilitate this, "tls-exporter" uses Exported Keying Material (EKM), which is already widely exposed by TLS implementations. The EKM is obtained using the keying material exporters for TLS, as defined in [RFC5705] and Section 7.5 of [RFC8446], by supplying the following inputs:

Label: The ASCII string "EXPORTER-Channel-Binding" with no terminating NUL.

Context value: Zero-length string.

Length: 32 bytes.

This channel binding mechanism is defined only when the TLS handshake results in unique master secrets. This is true of TLS versions prior to 1.3 when the extended master secret extension of [RFC7627] is in use, and it is always true for TLS 1.3 (see Appendix D of [RFC8446]).

3. TLS 1.3 with SCRAM or GSS-API over SASL

The specifications for Salted Challenge Response Authentication Mechanism (SCRAM) [RFC5802] [RFC7677] and Generic Security Service Application Program Interface (GSS-API) over Simple Authentication and Security Layer (SASL) [RFC5801] define "tls-unique" as the default channel binding to use over TLS. As "tls-unique" is not defined for TLS 1.3 (and greater), this document updates [RFC5801], [RFC5802], and [RFC7677] to use "tls-exporter" as the default channel binding over TLS 1.3 (and greater). Note that this document does not change the default channel binding for SCRAM mechanisms over TLS 1.2 [RFC5246], which is still "tls-unique" (also note that RFC 5246 has been obsoleted by RFC 8446).

Additionally, this document updates the aforementioned documents to make "tls-exporter" the mandatory-to-implement channel binding if any channel bindings are implemented for TLS 1.3. Implementations that support channel binding over TLS 1.3 MUST implement "tls-exporter".

4. Security Considerations

The channel binding type defined in this document is constructed so that disclosure of the channel binding data does not leak secret information about the TLS channel and does not affect the security of the TLS channel.

The derived data MUST NOT be used for any purpose other than channel

bindings as described in [RFC5056]. In particular, implementations MUST NOT use channel binding as a secret key to protect privileged information.

The Security Considerations sections of [RFC5056], [RFC5705], and [RFC8446] apply to this document.

4.1. Uniqueness of Channel Bindings

The definition of channel bindings in [RFC5056] defines the concept of a "unique" channel binding as being one that is unique to the channel endpoints and unique over time, that is, a value that is unique to a specific instance of the lower-layer security protocol. When TLS is the lower-layer security protocol, as for the channel binding type defined in this document, this concept of uniqueness corresponds to uniquely identifying the specific TLS connection.

However, a stronger form of uniqueness is possible, which would entail uniquely identifying not just the lower-layer protocol but also the upper-layer application or authentication protocol that is consuming the channel binding. The distinction is relevant only when there are multiple instances of an authentication protocol, or multiple distinct authentication protocols, that run atop the same lower-layer protocol. Such a situation is rare; most consumers of channel bindings establish an instance of the lower-layer secure protocol, run a single application or authentication protocol as the upper-layer protocol, then terminate both upper and lower-layer protocols. In this situation, the stronger form of uniqueness is trivially achieved, given that the channel binding value is unique in the sense of [RFC5056].

The channel binding type defined by this document provides only the weaker type of uniqueness, as per [RFC5056]; it does not achieve the stronger uniqueness per the upper-layer protocol instance described above. This stronger form of uniqueness would be useful in that it provides protection against cross-protocol attacks for the multiple authentication protocols running over the same instance of the lower-layer protocol, and it provides protection against replay attacks that seek to replay a message from one instance of an authentication protocol in a different instance of the same authentication protocol, again running over the same instance of the lower-layer protocol. Both of these properties are highly desirable when performing formal analysis of upper-layer protocols; if these properties are not provided, such formal analysis is essentially impossible. In some cases, one or both of these properties may already be provided by specific upper-layer protocols, but that is dependent on the mechanism(s) in question, and formal analysis requires that the property is provided in a generic manner across all potential upper-layer protocols that exist or might exist in the future.

Accordingly, applications that make use of the channel binding type defined in this document MUST NOT use the channel binding for more than one authentication mechanism instance on a given TLS connection. Such applications MUST immediately close the TLS connection after the conclusion of the upper-layer protocol.

4.2. Use with Legacy TLS

While it is possible to use this channel binding mechanism with TLS versions below 1.3, extra precaution must be taken to ensure that the chosen cipher suites always result in unique master secrets. For more information, see [RFC7627] and the Security Considerations section of [RFC5705] (TLS 1.3 always provides unique master secrets, as discussed in Appendix D of [RFC8446]).

When TLS renegotiation is enabled on a connection, the "tls-exporter" channel binding type is not defined for that connection, and implementations MUST NOT support it.

In general, users wishing to take advantage of channel binding should upgrade to TLS 1.3 or later.

5. IANA Considerations

5.1. Registration of Channel Binding Type

IANA has registered tls-exporter in the "Channel-Binding Types" registry:

Channel-binding unique prefix: tls-exporter

Channel-binding type: unique

Channel type: TLS [RFC8446]

Published specification: RFC 9266

Channel-binding is secret: no

Description: The EKM value obtained from the current TLS connection.

Intended usage: COMMON

Person and email address to contact for further information: Sam Whited <sam@samwhited.com>

Owner/Change controller name and email address: IESG

Expert reviewer name and contact information: IETF KITTEN WG <kitten@ietf.org> or IETF TLS WG <tls@ietf.org>

Note: See the published specification for advice on the applicability of this channel binding type.

5.2. Registration of Channel Binding TLS Exporter Label

IANA has added the following registration in the "TLS Exporter Labels" registry under the "Transport Layer Security (TLS) Parameters" registry:

Value: EXPORTER-Channel-Binding

DTLS-OK: Y

Recommended: Y

Reference: RFC 9266

6. References

6.1. 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>>.
- [RFC5056] Williams, N., "On the Use of Channel Bindings to Secure Channels", RFC 5056, DOI 10.17487/RFC5056, November 2007, <<https://www.rfc-editor.org/info/rfc5056>>.
- [RFC5705] Rescorla, E., "Keying Material Exporters for Transport Layer Security (TLS)", RFC 5705, DOI 10.17487/RFC5705, March 2010, <<https://www.rfc-editor.org/info/rfc5705>>.
- [RFC5801] Josefsson, S. and N. Williams, "Using Generic Security Service Application Program Interface (GSS-API) Mechanisms in Simple Authentication and Security Layer (SASL): The GS2 Mechanism Family", RFC 5801, DOI 10.17487/RFC5801, July 2010, <<https://www.rfc-editor.org/info/rfc5801>>.
- [RFC5802] Newman, C., Menon-Sen, A., Melnikov, A., and N. Williams,

"Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms", RFC 5802, DOI 10.17487/RFC5802, July 2010, <<https://www.rfc-editor.org/info/rfc5802>>.

[RFC5929] Altman, J., Williams, N., and L. Zhu, "Channel Bindings for TLS", RFC 5929, DOI 10.17487/RFC5929, July 2010, <<https://www.rfc-editor.org/info/rfc5929>>.

[RFC7677] Hansen, T., "SCRAM-SHA-256 and SCRAM-SHA-256-PLUS Simple Authentication and Security Layer (SASL) Mechanisms", RFC 7677, DOI 10.17487/RFC7677, November 2015, <<https://www.rfc-editor.org/info/rfc7677>>.

[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>>.

6.2. Informative References

[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>>.

[RFC7627] Bhargavan, K., Ed., Delignat-Lavaud, A., Pironti, A., Langley, A., and M. Ray, "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension", RFC 7627, DOI 10.17487/RFC7627, September 2015, <<https://www.rfc-editor.org/info/rfc7627>>.

[TRIPLE-HANDSHAKE]

Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Pironti, A., and P. Strub, "Triple Handshakes Considered Harmful: Breaking and Fixing Authentication over TLS", March 2014, <<https://www.mitls.org/pages/attacks/3SHAKE>>.

Author's Address

Sam Whited
Atlanta, GA
United States of America
Email: sam@samwhited.com
URI: <https://blog.samwhited.com/>