Workgroup: TLS Working Group
Internet-Draft:
draft-ietf-tls-cross-sni-resumption
Published: 15 December 2020
Intended Status: Standards Track
Expires: 18 June 2021
Authors: V. Vasiliev
Google

Transport Layer Security (TLS) Resumption across Server Names

Abstract

This document specifies a way for the parties in the Transport Layer Security (TLS) protocol to indicate that an individual session ticket can be used to perform resumption even if the Server Name of the new connection does not match the Server Name of the original.

Discussion Venues

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

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

Source for this draft and an issue tracker can be found at https://github.com/vasilvv/tls-cross-sni-resumption.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Transport Layer Security protocol [RFC8446] allows the clients to use an abbreviated handshake in cases where the client has previously established a secure session with the same server. This mechanism is known as "session resumption", and its positive impact on performance makes it desirable to be able to use it as frequently as possible.

Modern application-level protocols, HTTP in particular, often require accessing multiple servers within a single workflow. Since the identity of the server is established through its certificate, in the ideal case, the resumption would be possible to all of the domains for which the certificate is valid (see [PERF] for a survey of potential practical impact of such approach). TLS, starting with version 1.3, defines the SNI value to be a property of an individual connection that is not retained across sessions ([RFC8446], Section 4.2.11). However, in the absence of additional signals, it discourages using a session ticket when the SNI value does not match ([RFC8446], Section 4.6.1), as there is normally no reason to assume that all servers sharing the same certificate would also share the same session keys. The extension defined in this document allows the server to provide such a signal in-band.

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. The Extension

The server MAY send a resumption_across_names(TBD) extension in a NewSessionTicket message. That extension SHALL have an empty body. If the extension is sent, it indicates that the client MAY use the ticket for any SNI value for which the certificate presented by the server is valid. The server MUST handle the ticket correctly by either resuming and using a new SNI provided by the client, or by ignoring the ticket.

The server MAY send the extension if it reasonably believes that any server for any identity presented in its certificate would be capable of accepting that ticket. The server SHOULD NOT send the extension otherwise, since, if the client follows the single-use ticket policy recommended by [RFC8446], sending the ticket results in it being no longer usable regardless of whether resumption has succeeded.

4. Security Considerations

This document does not alter any of the security requirements of [RFC8446], but merely lifts a performance-motivated "SHOULD NOT" recommendation from Section 4.6.1. Notably, it still relies on the server certificate being re-validated against the new SNI at the session resumption time.

If a client certificate has been associated with the session, the client MUST use the same policy on whether to present said certificate to the server as if it were a new TLS session. For instance, if the client would show a certificate choice prompt for every individual domain it connects to, it MUST show that prompt for the new host when performing cross-domain resumption.

Cross-domain resumption, like other similar mechanisms (e.g. cross-domain HTTP connection reuse), can incentivize the server deployments to create server certificates valid for a wider range of domains than they would otherwise. However, any increase in the scope of a certificate comes at a cost: the wider is the scope of the certificate, the wider is the impact of the key compromise for that certificate. In addition, creating a certificate that is valid for multiple hostnames can lead to complications if some of those hostnames change ownership, or otherwise require a different operational domain.

Session tickets can contain arbitrary information, and thus could be potentially used to re-identify a user from a previous connection. Cross-domain resumption expands the potential list of servers to which an individual ticket could be presented. Client applications should partition the session cache between connections that are meant to be uncorrelated. For example, the Web use case uses network partition keys to separate cache lookups [FETCH].

5. IANA Considerations

IANA (will add/has added) the following entry to the "TLS ExtensionType Values" table of the "Transport Layer Security (TLS) Extensions" registry:

Value TBD

Extension Name resumption_across_names

TLS 1.3 NST

Recommended N

Reference This document

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>.

[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

[FETCH] WHATWG, "Fetch Standard", December 2020, <https://fetch.spec.whatwg.org/>.

[PERF] Sy, E., Moennich, M., Mueller, T., Federrath, H., and M. Fischer, "Enhanced Performance for the encrypted Web through TLS Resumption across Hostnames", 7 February 2019, <https://arxiv.org/pdf/1902.02531.pdf>.

Acknowledgments

Cross-name resumption has been previously implemented in the QUIC Crypto protocol as a preloaded list of hostnames.

Erik Sy has previously proposed a similar mechanism for TLS, draft-sy-tls-resumption-group. This document incorporates ideas from that draft.

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

Author's Address

Victor Vasiliev
Google

Email: vasilvv@google.com