Network Working Group
Internet-Draft
Updates: 4572 (if approved)
Intended status: Standards Track
Expires: November 22, 2016

C. Holmberg
Ericsson

May 21, 2016

Updates to RFC 4572
draft-ietf-mmusic-4572-update-03.txt

Abstract

This document updates RFC 4572 by clarifying the usage of multiple SDP 'fingerprint' attributes with a single TLS connection. The document also updates the preferred cipher suite to be used, and removes the requirement to use the same hash function for calculating a certificate fingerprint that is used to calculate the certificate signature.

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 November 22, 2016.

Table of Contents

1. Introduction

RFC 4572 [RFC4572] specifies how to establish Transport Layer Security (TLS) connections using the Session Description Protocol (SDP) [RFC4566].

RFC 4572 defines the SDP 'fingerprint' attribute, which is used to carry a secure hash value (fingerprint) associated with a certificate. However, RFC 4572 is currently unclear on whether multiple 'fingerprint' attributes can be associated with a single SDP media description ("m= line") [RFC4566], and the associated semantics. Multiple fingerprints are needed if an endpoints wants to provide fingerprints associated with multiple certificates. For example, with RTP-based media, an endpoint might use different certificates for RTP and RTCP.

RFC 4572 also specifies a preferred cipher suite. However, the currently preferred cipher suite is considered outdated, and the preference needs to be updated.

RFC 4572 mandates that the hash function used to calculate the fingerprint is the same hash function used to calculate the certificate signature. That requirement might prevent usage of newer, stronger and more collision-safe hash functions for calculating certificate fingerprints. This change also requires that multiple 'fingerprint' attributes can be associated with a single "m=" line, so that implementations are able to provide fingerprints calculated using updated hash functions alongside those that are needed to interoperate with existing implementations.

This document updates RFC 4572 [RFC4572] by clarifying the usage of multiple SDP 'fingerprint' attributes. It is clarified that multiple 'fingerprint' attributes can be used to carry fingerprints, calculated using different hash functions, associated with a given certificate, and to carry fingerprints associated with multiple certificates. The fingerprint matching procedure, when multiple fingerprints are provided, are also clarified. The document also updates the preferred cipher suite to be used, and removes the requirement to use the same hash function for calculating a certificate fingerprint and certificate signature.

2. Conventions

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. Update to RFC 4572

This section updates section 5 of RFC 4572.

3.1. Update to the sixth paragraph of section 5

OLD TEXT:

> A certificate fingerprint MUST be computed using the same one-way hash function as is used in the certificate's signature algorithm. (This ensures that the security properties required for the certificate also apply for the fingerprint. It also guarantees that the fingerprint will be usable by the other endpoint, so long as the certificate itself is.) Following RFC 3279 [7] as updated by RFC 4055 [9], therefore, the defined hash functions are 'SHA-1' [11] [19], 'SHA-224' [11], 'SHA-256' [11], 'SHA-384' [11], 'SHA-512' [11] , 'MD5' [12], and 'MD2' [13], with 'SHA-1' preferred. A new IANA registry of Hash Function Textual Names, specified in Section 8, allows for addition of future tokens, but they may only be added if they are included in RFCs that update or obsolete RFC 3279 [7]. Self-signed certificates (for which legacy certificates are not a consideration) MUST use one of the FIPS 180 algorithms (SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512) as their signature algorithm, and thus also MUST use it to calculate certificate fingerprints.

NEW TEXT:

> Following RFC 3279 [7] as updated by RFC 4055 [9], therefore, the defined hash functions are 'SHA-1' [11] [19], 'SHA-224' [11], 'SHA-256' [11], 'SHA-384' [11], 'SHA-512' [11], 'MD5' [12], and 'MD2' [13], with 'SHA-256' preferred. A new IANA registry of Hash Function Textual Names, specified in Section 8, allows for addition of future tokens, but they may only be added if they are included in RFCs that update or obsolete RFC 3279 [7].

3.2. New paragraphs to the end of section 5

NEW TEXT:

> Multiple SDP fingerprint attributes can be associated with an m-line. This can occur if multiple fingerprints have been calculated for a certificate using different hash functions. It can also occur if one or more fingerprints associated with multiple certificates have been calculated. This might be needed if multiple certificates will be used for media associated with an m- line (e.g. if separate certificates are used for RTP and RTCP), or where it is not known which certificate will be used when the fingerprints are exchanged. In such cases, one or more fingerprints MUST be calculated for each possible certificate.
>
> If fingerprints associated with multiple certificates are calculated, the same set of hash functions MUST be used to calculate fingerprints for each certificate associated with the m- line.
>
> For each used certificate, an endpoint MUST be able to match at least one fingerprint, calculated using the hash function that the endpoint supports and considers most secure, with the used certificate. If there is no match, the endpoint MUST NOT establish the TLS connection. In addition, the endpoint MAY also check fingerprints calculated using other hash functions that it has received for a match. For each hash function checked, one of the received fingerprints MUST match the used certificate.
>
> NOTE: The SDP fingerprint attribute does not contain a reference to a specific certificate. Endpoints need to compare the fingerprint with a certificate hash in order to look for a match.

4. Security Considerations

This document improves security. It updates the preferred hash function cipher suite from SHA-1 to SHA-256. By clarifying the usage and handling of multiple fingerprints, the document also enables hash agility, and incremental deployment of newer, and more secure, cipher suites.

5. IANA Considerations

This document makes no requests from IANA.

6. Acknowledgements

Martin Thomson, Paul Kyzivat, Jonathan Lennox and Roman Shpount provided valuable comments and input on this document.

7. Change Log

[RFC EDITOR NOTE: Please remove this section when publishing]

Changes from draft-ietf-mmusic-4572-update-02

- Editorial fixes based on comments from Martin Thomson.
- Non-used references removed.

Changes from draft-ietf-mmusic-4572-update-01

- Changes based on comments from Martin Thomson.
- - Editorial fixes
- Changes in handling of multiple fingerprints.
- - Sender must send same set of hash functions for each offered certificate.
- - Receiver must check the hash function it considers most secure for a match. It may check other hash functions.

Changes from draft-ietf-mmusic-4572-update-00

- Changes in handling of multiple fingerprints.
- - Number of fingerprints calculated for each certificate does not have to match.
- - Clarified that receiver shall check check fingerprints using hash algorithms it considers safe.
- - Additional text added to security considerations section.

Changes from draft-holmberg-mmusic-4572-update-01

- Adopted WG document (draft-ietf-mmusic-4572-update-00) submitted.
- IANA considerations section added.

8. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4572] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, DOI 10.17487/RFC4572, July 2006, <http://www.rfc-editor.org/info/rfc4572>.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, DOI 10.17487/RFC4566, July 2006, <http://www.rfc-editor.org/info/rfc4566>.

Author's Address

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: christer.holmberg@ericsson.com