

TLS
Internet-Draft
Updates: [10000](#) (if approved)
Intended status: Standards Track
Expires: November 16, 2018

Alan Smithee

Alan Smithee
May 15, 2018

TLS Downgrade protection extension for TLS DNSSEC Authentication Chain
Extension
draft-asmithee-tls-dnssec-downprot-00

Abstract

This draft specifies a TLS extension that adds downgrade protection for another TLS extension, [[dnssec-chain-extension](#)]. Without the downgrade protection specified in this TLS extension, the only effect of deploying [[dnssec-chain-extension](#)] is to reduce TLS security from the standard "WebPKI security" to "WebPKI or DANE, whichever is weaker".

This draft dictates that [[dnssec-chain-extension](#)] MUST only be used in combination with this TLS extension, whose only content is a two octet SupportLifetime value. A value of 0 prohibits the TLS client from unilaterally requiring ongoing use of both TLS extensions based on prior observation of their use (pinning). A non-zero value is the value in hours for which this TLS extension as well as [[dnssec-chain-extension](#)] MUST appear in subsequent TLS handshakes to the same TLS hostname and port. If this TLS extension or [[dnssec-chain-extension](#)] is missing from the TLS handshake within this observed pinning time, the TLS client MUST assume it is under attack and abort the TLS connection.

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 16, 2018.

Copyright Notice

Copyright (c) 2018 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 (<http://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 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.	Requirements Notation	2
2.	Introduction	2
3.	TLS DNSSEC Extension Downgrade Protection Extension format .	3
4.	Operational Considerations	3
5.	Security Considerations	4
6.	IANA Considerations	4
7.	Normative References	4
	Authors' Addresses	5

[1.](#) Requirements Notation

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.](#) Introduction

This draft specifies a TLS extension that adds downgrade protection for another TLS extension, [[dnssec-chain-extension](#)]. Without the downgrade protection specified in this TLS extension, the only effect of deploying [[dnssec-chain-extension](#)] is to reduce TLS security from the standard "WebPKI security" to "WebPKI or DANE, whichever is weaker".

This draft dictates that [[dnssec-chain-extension](#)] MUST only be used in combination with this TLS extension, whose only content is a two byte SupportLifetime value. A value of 0 prohibits the TLS client from unilaterally requiring ongoing use of both TLS extensions based on prior observation of their use (pinning). A non-zero value is the

value in hours for which this TLS extension as well as [[dnssec-chain-extension](#)] MUST appear in subsequent TLS handshakes to the same hostname and port. If this TLS extension or [[dnssec-chain-extension](#)] is missing from the TLS handshake within this observed pinning time, the TLS client MUST assume it is under attack and abort the TLS connection.

3. TLS DNSSEC Extension Downgrade Protection Extension format

The "extension_data" field of the "dnssec_chain_commit" extension contains a two octet value specifying the pinning time in hours for both this extension and [[dnssec-chain-extension](#)] in the following form:

```
struct {  
    uint16 SupportLifetime;  
} DnssecChainExtensionCommitTime;
```

A zero "SupportLifetime" prohibits the client from unilaterally requiring ongoing use of this extension or [[dnssec-chain-extension](#)] based on prior observation of their use (pinning).

A non-zero value signifies the time in hours for which this resource commits to publishing both this extension and [[dnssec-chain-extension](#)]. If within the specified time a TLS connection for this resource omits either TLS extension, the TLS client MUST conclude it is under attack and MUST abort the TLS connection.

4. Operational Considerations

A positive DANE validated response for the TLSA record in [[dnssec-chain-extension](#)] MUST override any previous SupportLifetime information that the TLS client stored previously. In addition, if the TLS client previously obtained a valid TLSA record with a SupportLifetime commitment further into the future, and as part of

the current TLS handshake it receives a DNSSEC-validated answer containing no TLSA record and a Denial of Existence proof via [\[dnssec-chain-extension\]](#), the TLS client MUST clear the previously stored TLS extensions pinning value.

If a specific resource is served using multiple TLS servers or clusters, and a non-zero value for SupportLifetime is used, all TLS server instances MUST support serving both this extension and [\[dnssec-chain-extension\]](#). As long as no TLS service instance uses a non-zero value, both TLS extensions can be rolled out incrementally without any TLS clients committing to either TLS extension.

[5.](#) Security Considerations

This draft specifies a TLS extension that adds downgrade protection for another TLS extension, [\[dnssec-chain-extension\]](#). Without the downgrade protection specified in this TLS extension, the only effect of deploying [\[dnssec-chain-extension\]](#) is to reduce TLS security from the standard "WebPKI security" to "WebPKI or DANE, whichever is weaker".

This draft dictates that [\[dnssec-chain-extension\]](#) MUST only be used in combination with this TLS extension, whose only content is a two byte SupportLifetime value. A value of 0 prohibits the TLS client from unilaterally requiring ongoing use of both TLS extensions based on prior observation of their use (pinning). A non-zero value is the value in hours for which this TLS extension as well as [\[dnssec-chain-extension\]](#) MUST appear in subsequent TLS handshakes to the same hostname and port. If this TLS extension or [\[dnssec-chain-extension\]](#) is missing from the TLS handshake within this observed pinning time, the TLS client MUST assume it is under attack and abort the TLS connection.

[6.](#) IANA Considerations

This extension requires the registration of a new value in the TLS ExtensionsType registry. The value requested from IANA is [TBD], and the extension should be marked "Recommended" in accordance with "IANA Registry Updates for TLS and DTLS" [\[TLSIANA\]](#).

[7.](#) 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>>.
- [dnssec-chain-extension] Shore, M., Barnes, R., Hugue, S., and W. Toorop, "A DANE Record and DNSSEC Authentication Chain Extension for TLS", March 2018, <<https://tools.ietf.org/html/draft-ietf-tls-dnssec-chain-extension-07>>.
- [TLSIANA] Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", <<https://tools.ietf.org/html/draft-ietf-tls-iana-registry-updates>>.

Alan Smithee & Alan SmitExpires November 16, 2018

[Page 4]

Internet-Draft TLS DNSSEC Chain Downgrade Protection

May 2018

Authors' Addresses

Alan Smithee

EMail: pwouters@redhat.com

Alan Smithee

EMail: ietf-dane@dukhovni.org

