LAMPS
Internet-Draft
Intended status: Standards Track
Expires: October 25, 2020

M. Sahni, Ed.
Palo Alto Networks

April 23, 2020

OCSP Nonce Extension
draft-ietf-lamps-ocsp-nonce-00

Abstract

This document specifies the updated format of the Nonce extension in Online Certificate Status Protocol (OCSP) request and response messages. OCSP is used to check the status of a certificate and the Nonce extension is used in the OCSP request and response messages to avoid replay attacks. This document updates the RFC 6960

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 https://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 October 25, 2020.

Table of Contents

1. Introduction

This document updates the usage and format of the Nonce extension used in OCSP request and response messages. This extension was previously defined in section 4.1.1 of [RFC6960]. The [RFC6960] does not mention any minimum and maximum length of the nonce extension. Due to not having an upper or lower limit of the length of the Nonce extension, the OCSP responders that follow [RFC6960] may be vulnerable to various attacks like Denial of Service attacks [RFC4732], chosen prefix attacks to get a desired signature from the OCSP responder and possible evasions that can use the Nonce extension data for evasion. This document specifies a lower limit of 1 and an upper limit of 32 to the length of the Nonce extension. This document updates the [RFC6960].

1.1. Terminology

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. OCSP Extensions

The message format for the OCSP request and response is defined in the [RFC6960]. It also defines the standard extensions for OCSP messages based on the extension model employed in X.509 version 3 certificates (see [RFC5280]). Following is the list of standard

extensions that can be used in the OCSP messages by the OCSP responder and OCSP client.

* Nonce
* CRL References
* Acceptable Response Types
* Archive Cutoff
* CRL Entry Extensions
* Service Locator
* Preferred Signature Algorithms
* Extended Response Definition

This document only specifies the new format for Nonce extension and does not change the specification of any of the other standard extensions.

2.1. Nonce Extension

This section updates the Section 4.4.1 [1] of [RFC6960] which describes the OCSP Nonce extension.

The nonce cryptographically binds a request and a response to prevent replay attacks. The nonce is included as one of the requestExtensions in requests, while in responses it would be included as one of the responseExtensions. In both the request and the response, the nonce will be identified by the object identifier id-pkix-ocsp-nonce, while the extnValue is the value of the nonce. If Nonce extension is present then the length of nonce MUST be at least 1 octet and can be up to 32 octets.

A server MUST reject any OCSP request having a Nonce extension with length of more than 32 octets with the malformedRequest OCSPResponseStatus as described in section 4.2.1 of [RFC6960]

The minimum nonce length of 1 octet is defined to provide the backward compatibility with clients following [RFC6960]. However the newer OCSP clients MUST use length of at least 16 octets for Nonce extension and the value of the nonce MUST be generated using a cryptographically strong pseudorandom number generator.

```
id-pkix-ocsp           OBJECT IDENTIFIER ::= { id-ad-ocsp }

id-pkix-ocsp-nonce     OBJECT IDENTIFIER ::= { id-pkix-ocsp 2 }

Nonce ::= OCTET STRING(SIZE(1..32))
```

3. Security Considerations

The security considerations of OCSP, in general, are described in the [RFC6960]. The Nonce extension is used to avoid replay attacks during the interval in which the previous OCSP response for a certificate is not expired but the responder has a changed status for that certificate. Including client's Nonce value in the OCSP response makes sure that the response is the latest response from the server and not an old copy.

3.1. Replay Attack

The Nonce extension is used to avoid replay attacks. Since the OCSP responder may choose to not send the Nonce extension in the OCSP response even if the client has sent the Nonce extension in the request [RFC5019], a man in the middle (MITM) entity can intercept the OCSP request and respond with an earlier response from the server without the Nonce extension. This can be mitigated by the server using a closer nextUpdate value in the OCSP response.

3.2. Nonce Collision

If the value of the nonce used by a client is not random enough, then an attacker may prefetch responses with the predicted nonce and can replay them, thus defeating the purpose of using nonce. Therefore the client MUST use a nonce value that contains cryptographically strong randomness and is freshly generated. Also if the length of the nonce is very small e.g. 1 octet then an attacker can prefetch responses with all the possible values of the nonce and replay a matching nonce. A client SHOULD use 32 octets for the nonce length.

4. IANA Considerations

This document does not include any new media type registrations for OCSP.

5. Changes to Appendix B. of RFC 6960

This section updates the ASN.1 definitions of the OCSP Nonce extension in the Appendix B.1 and Appendix B.2 of the [RFC6960] The Appendix B.1 defines OCSP using ASN.1 - 1998 Syntax and Appendix B.2 defines OCSP using ASN.1 - 2008 Syntax

5.1. Changes to Appendix B.1. OCSP in ASN.1 - 1998 Syntax

OLD Syntax:

The definition of OCSP Nonce Extension is not provided in the Appendix B.1 of [RFC6960] for the ASN.1 - 1998 Syntax.

NEW Syntax:

```
Nonce ::= OCTET STRING(SIZE(1..32))
```

5.2. Changes to Appendix B.2 OCSP in ASN.1 - 2008 Syntax

OLD Syntax:

```
re-ocsp-nonce EXTENSION ::= { SYNTAX OCTET STRING IDENTIFIED
    BY id-pkix-ocsp-nonce }
```

NEW Syntax:

```
re-ocsp-nonce EXTENSION ::= { SYNTAX OCTET STRING(SIZE(1..32))
    IDENTIFIED BY id-pkix-ocsp-nonce }
```

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

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", DOI 10.17487/RFC8174, RFC 8174, BCP 14, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, DOI 10.17487/RFC6960, June 2013, <https://www.rfc-editor.org/info/rfc6960>.

6.2. Informative References

[RFC4732] Handley, M., Ed., Rescorla, E., Ed., and IAB, "Internet Denial-of-Service Considerations", RFC 4732, DOI 10.17487/RFC4732, December 2006, <https://www.rfc-editor.org/info/rfc4732>.

[RFC5019] Deacon, A. and R. Hurst, "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments", RFC 5019, DOI 10.17487/RFC5019, September 2007, <https://www.rfc-editor.org/info/rfc5019>.

6.3. URIs

[1] https://tools.ietf.org/html/rfc6960#section-4.4.1

Author's Address

Mohit Sahni (editor)
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
US

Email: msahni@paloaltonetworks.com