Network Working Group
Request for Comments: 4806
Category: Standards Track

M. Myers
TraceRoute Security LLC
H. Tschofenig
Siemens Networks GmbH & Co KG

February 2007

Online Certificate Status Protocol (OCSP) Extensions to IKEv2

Status of This Memo

Copyright Notice

Abstract

While the Internet Key Exchange Protocol version 2 (IKEv2) supports public key based authentication, the corresponding use of in-band Certificate Revocation Lists (CRL) is problematic due to unbounded CRL size. The size of an Online Certificate Status Protocol (OCSP) response is however well-bounded and small. This document defines the "OCSP Content" extension to IKEv2. A CERTREQ payload with "OCSP Content" identifies zero or more trusted OCSP responders and is a request for inclusion of an OCSP response in the IKEv2 handshake. A cooperative recipient of such a request responds with a CERT payload containing the appropriate OCSP response. This content is recognizable via the same "OCSP Content" identifier.

When certificates are used with IKEv2, the communicating peers need a mechanism to determine the revocation status of the peer's certificate. OCSP is one such mechanism. This document applies when OCSP is desired and security policy prevents one of the IKEv2 peers from accessing the relevant OCSP responder directly. Firewalls are often deployed in a manner that prevents such access by IKEv2 peers outside of an enterprise network.

Table of Contents

1. Introduction

Version 2 of the Internet Key Exchange (IKE) protocol [IKEv2] supports a range of authentication mechanisms, including the use of public key based authentication. Confirmation of certificate reliability is essential in order to achieve the security assurances public key cryptography provides. One fundamental element of such confirmation is reference to certificate revocation status (see [RFC3280] for additional detail).

The traditional means of determining certificate revocation status is through the use of Certificate Revocation Lists (CRLs). IKEv2 allows CRLs to be exchanged in-band via the CERT payload.

However, CRLs can grow unbounded in size. Many real-world examples exist to demonstrate the impracticality of including a multi-megabyte file in an IKE exchange. This constraint is particularly acute in bandwidth-limited environments (e.g., mobile communications). The net effect is exclusion of in-band CRLs in favor of out-of-band (OOB) acquisition of these data, should they even be used at all.

Reliance on OOB methods can be further complicated if access to revocation data requires use of IPsec (and therefore IKE) to establish secure and authorized access to the CRLs of an IKE participant. Such network access deadlock further contributes to a reduced reliance on the status of certificate revocations in favor of blind trust.

OCSP [RFC2560] offers a useful alternative. The size of an OCSP response is bounded and small and therefore suitable for in-band IKEv2 signaling of a certificate's revocation status.

This document defines an extension to IKEv2 that enables the use of OCSP for in-band signaling of certificate revocation status. A new content encoding is defined for use in the CERTREQ and CERT payloads. A CERTREQ payload with "OCSP Content" identifies zero or more trusted OCSP responders and is a request for inclusion of an OCSP response in the IKEv2 handshake. A cooperative recipient of such a request responds with a CERT payload containing the appropriate OCSP response. This content is recognizable via the same "OCSP Content" identifier.

2. Terminology

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 RFC 2119 [RFC2119].

This document defines the following terms:

OCSP request:

> An OCSP request refers to the CERTREQ payload that contains a new content encoding, referred to as OCSP Content, that conforms to the definition and behavior specified in Section 3.1.

OCSP response:

> An OCSP response refers to the CERT payload that contains a new content encoding, referred to as OCSP Content, that conforms to the definition and behavior specified in Section 3.2.

OCSP responder:

> The term OCSP responder refers to the entity that accepts requests from an OCSP client and returns responses as defined in [RFC2560]. Note that the OCSP responder does not refer to the party that sends the CERT message.

3. Extension Definition

With reference to Section 3.6 of [IKEv2], the values for the Cert Encoding field of the CERT payload are extended as follows (see also the IANA Considerations section of this document):

Certificate Encoding	Value
OCSP Content	14

3.1. OCSP Request

A value of OCSP Content (14) in the Cert Encoding field of a CERTREQ Payload indicates the presence of zero or more OCSP responder certificate hashes in the Certificate Authority field of the CERTREQ payload. Section 2.2 of [RFC2560] defines responses, which belong to one of the following three groups:

(a) the CA who issued the certificate

(b) a Trusted Responder whose public key is trusted by the requester

(c) a CA Designated Responder (Authorized Responder) who holds a specially marked certificate issued directly by the CA, indicating that the responder may issue OCSP responses for that CA

In case of (a), the use of hashes in the CERTREQ message is not needed since the OCSP response is signed by the CA who issued the certificate. In case of (c), the OCSP response is signed by the CA Designated Responder whereby the sender of the CERTREQ message does not know the public key in advance. The presence of OCSP Content in a CERTREQ message will identify one or more OCSP responders trusted by the sender in case of (b).

The presence of OCSP Content (14) in a CERTREQ message:

1. identifies zero or more OCSP responders trusted by the sender;

2. notifies the recipient of sender’s support for the OCSP extension to IKEv2; and

3. notifies the recipient of sender’s desire to receive OCSP confirmation in a subsequent CERT payload.

3.2. OCSP Response

A value of OCSP Content (14) in the Cert Encoding field of a CERT Payload indicates the presence of an OCSP response in the Certificate Data field of the CERT payload.

Correlation between an OCSP response CERT payload and a corresponding CERT payload carrying a certificate can be achieved by matching the OCSP response CertID field to the certificate. See [RFC2560] for the definition of OCSP response content.

4. Extension Requirements

4.1. Request for OCSP Support

Section 3.7 of [IKEv2] allows for the concatenation of trust anchor hashes as the Certification Authority value of a single CERTREQ message. There is no means however to indicate which among those hashes, if present, relates to the certificate of a trusted OCSP responder.

Therefore, an OCSP request, as defined in Section 3.1 above, is transmitted separate from any other CERTREQ payloads in an IKEv2 exchange.

Where it is useful to identify more than one trusted OCSP responder, each such identification SHALL be concatenated in a manner identical to the method documented in Section 3.7 of [IKEv2] regarding the assembly of multiple trust anchor hashes.

The Certification Authority value in an OCSP request CERTREQ SHALL be computed and produced in a manner identical to that of trust anchor hashes as documented in Section 3.7 of [IKEv2].

Upon receipt of an OCSP response CERT payload corresponding to a prior OCSP request CERTREQ, the CERTREQ sender SHALL incorporate the OCSP response into path validation logic defined by [RFC3280].

Note that the lack of an OCSP response CERT payload after sending an OCSP request CERT payload might be an indication that this OCSP extension is not supported. As a result, it is recommended that nodes be configured to require a response only if it is known that all peers do in fact support this extension. Otherwise, it is recommended that the nodes be configured to try OCSP and, if there is no response, attempt to determine certificate revocation status by some other means.

4.2. Response to OCSP Support

Upon receipt of an OCSP request CERTREQ payload, the recipient SHOULD acquire the related OCSP-based assertion and produce and transmit an OCSP response CERT payload corresponding to the certificate needed to verify its signature on IKEv2 payloads.

An OCSP response CERT payload is transmitted separate from any other CERT payload in an IKEv2 exchange.

The means by which an OCSP response may be acquired for production of an OCSP response CERT payload is out of scope of this document.

The Certificate Data field of an OCSP response CERT payload SHALL contain a DER-encoded OCSPResponse structure as defined in [RFC2560].

5. Examples and Discussion

This section shows the standard IKEv2 message examples with both peers, the initiator and the responder, using public key based authentication, CERTREQ and CERT payloads. The first instance corresponds to Section 1.2 of [IKEv2], the illustrations of which are reproduced below for reference.

5.1. Peer to Peer

Application of the IKEv2 extensions defined in this document to the peer-to-peer exchange defined in Section 1.2 of [IKEv2] is as follows. Messages are numbered for ease of reference.

```
     Initiator                              Responder
     -----------                            -----------
(1)  HDR, SAi1, KEi, Ni             -->

(2)                                 <-- HDR, SAr1, KEr, Nr,
                                        CERTREQ(OCSP Request)
(3)  HDR, SK {IDi, CERT(certificate),-->
     CERT(OCSP Response),
     CERTREQ(OCSP Request),
     [IDr,] AUTH, SAi2, TSi, TSr}

(4)                                 <-- HDR, SK {IDr,
                                        CERT(certificate),
                                        CERT(OCSP Response),
                                        AUTH, SAr2, TSi, TSr}
```

OCSP Extensions to Baseline IKEv2

In (2), Responder sends an OCSP request CERTREQ payload identifying zero or more OCSP responders trusted by the Responder. In response, Initiator sends in (3) both a CERT payload carrying its certificate and an OCSP response CERT payload covering that certificate. In (3), Initiator also requests an OCSP response via the OCSP request CERTREQ payload. In (4), the Responder returns its certificate and a separate OCSP response CERT payload covering that certificate.

It is important to note that in this scenario, the Responder in (2) does not yet possess the Initiator's certificate and therefore cannot form an OCSP request as defined in [RFC2560]. To bypass this problem, hashes are used as defined in Section 4.1. In such instances, OCSP Requests are simply index values into these data. Thus, it is easily inferred that OCSP responses can be produced in the absence of a corresponding request (provided that OCSP nonces are not used, see Section 6).

It is also important in extending IKEv2 toward OCSP in this scenario that the Initiator has certain knowledge that the Responder is capable of and willing to participate in the extension. Yet the Responder will only trust one or more OCSP responder signatures. These factors motivate the definition of OCSP responder hash extension.

5.2. Extended Authentication Protocol (EAP)

Another scenario of pressing interest is the use of EAP to accommodate multiple end users seeking enterprise access to an IPsec gateway. Note that OCSP is used for the certificate status check of the server side IKEv2 certificate and not for certificates that may be used within EAP methods (either by the EAP peer or the EAP server). As with the preceding section, the following illustration is extracted from [IKEv2]. In the event of a conflict between this document and [IKEv2] regarding these illustrations, [IKEv2] SHALL dominate.

```
     Initiator                              Responder
     -----------                            -----------
(1)  HDR, SAi1, KEi, Ni                 -->
(2)                                     <-- HDR, SAr1, KEr, Nr
(3)  HDR, SK {IDi,                      -->
     CERTREQ(OCSP Request),
     [IDr,] AUTH, SAi2, TSi, TSr}
(4)                                     <-- HDR, SK {IDr,
                                            CERT(certificate),
                                            CERT(OCSP Response),
                                            AUTH, EAP}
(5)       HDR, SK {EAP}                 -->

(6)                                     <-- HDR, SK {EAP (success)}

(7)       HDR, SK {AUTH}                -->

(8)                                     <-- HDR, SK {AUTH, SAr2, TSi,
                                            TSr }
```

OCSP Extensions to EAP in IKEv2

In the EAP scenario, messages (5) through (8) are not relevant to this document.

6. Security Considerations

For the reasons noted above, an OCSP request, as defined in Section 3.1, is used in place of an OCSP request syntax to trigger production and transmission of an OCSP response. OCSP, as defined in [RFC2560], may contain a nonce request extension to improve security against replay attacks (see Section 4.4.1 of [RFC2560] for further details). The OCSP request defined by this document cannot accommodate nonces. [RFC2560] deals with this aspect by allowing pre-produced responses.

[RFC2560] points to this replay vulnerability and indicates: "The use of precomputed responses allows replay attacks in which an old (good) response is replayed prior to its expiration date but after the certificate has been revoked. Deployments of OCSP should carefully evaluate the benefit of precomputed responses against the probability of a replay attack and the costs associated with its successful execution." Nodes SHOULD make the required freshness of an OCSP response configurable.

7. IANA Considerations

This document defines one new field type for use in the IKEv2 Cert Encoding field of the Certificate Payload format. Official assignment of the "OCSP Content" extension to the Cert Encoding table of Section 3.6 of [IKEv2] has been acquired from IANA.

Certificate Encoding	Value
OCSP Content	14

8. Acknowledgements

The authors would like to thank Russ Housley for his support. Additionally, we would like to thank Pasi Eronen, Nicolas Williams, Liqiang (Larry) Zhu, Lakshminath Dondeti, and Paul Hoffman for their review. Pasi gave us invaluable last-call comments. We would also like to thank Tom Taylor for his Gen-ART review. Jari Arkko gave us IESG review comments.

9. Normative References

[IKEv2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

Authors' Addresses

Michael Myers
TraceRoute Security LLC

EMail: mmyers@fastq.com

Hannes Tschofenig
Siemens Networks GmbH & Co KG
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

EMail: Hannes.Tschofenig@siemens.com
URI: http://www.tschofenig.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.