OCSP Extensions to IKEv2

draft-myers-ipsec-ikev2-oscp-01.txt

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 31, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

While IKEv2 supports public key based authentication (PKI), the corresponding use of in-band CRLs is problematic due to unbounded CRL size. The size of an OCSP response is however well-bounded and small. This document defines two extensions to IKEv2 which enable the use of OCSP for in-band signaling of certificate revocation status. Two new content encodings are defined for use in the CERTREQ and CERT payloads: OCSP Responder Hash and OCSP Response. An OCSP Responder Hash CERTREQ payload triggers transmission of an OCSP Response CERT payload.

When certificates are used with IKEv2, the communicating peers need a mechanism to determine the revocation status of the peer’s certificate. OCSP [RFC2560] 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.
1. Introduction

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

The historic 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.

CRLs can however 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 certificate revocation status 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 two extensions to IKEv2 that enable the use of OCSP for in-band signaling of certificate revocation status. Two new content encodings are defined for use in the CERTREQ and CERT payloads: OCSP Responder Hash and OCSP Response. An OCSP Responder Hash CERTREQ payload triggers transmission of an OCSP Response CERT payload.

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 [RFC2119].

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):

<table>
<thead>
<tr>
<th>Certificate Encoding</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCSP Responder Hash</td>
<td>14</td>
</tr>
<tr>
<td>OCSP Response</td>
<td>15</td>
</tr>
</tbody>
</table>
3.1 OCSP Responder Hash

A value of OCSP Responder Hash (14) in the Cert Encoding field of a CERTREQ Payload indicates the presence of an OCSP Responder certificate hash in the Certificate Authority field of the CERTREQ payload.

The presence of the OCSP Responder Hash in a CERTREQ message:

1. identifies an OCSP responder 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 Response (15) 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

[IKEv2] allows for multiple CERT and CERTREQ payloads in an exchange.

4.1 OCSP Responder Hash

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 relates to the certificate of a trusted OCSP responder.

Therefore an OCSP Responder Hash CERTREQ SHALL be 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 transmitted via separate OCSP Responder Hash CERTREQ payloads.

The Certification Authority value in an OCSP Responder CERTREQ SHALL be computed and produced in a manner identical to that of trust anchor hashes as documented in Section 3.7 of [IKEv2] with the exception that each such hash SHALL be expressed in a separate CERTREQ payload.
Upon receipt of an OCSP Response CERT payload corresponding to a prior OCSP Responder Hash CERTREQ, the CERTREQ sender SHALL incorporate the OCSP response into path validation logic defined by [RFC3280].

The sender of an OCSP Responder Hash CERTREQ SHALL abort an IKEv2 exchange if either:

1. the corresponding OCSP Response CERT payload indicates that the subject certificate is revoked;
2. the corresponding OCSP Response CERT payload indicates an OCSP error (e.g. malformedRequest, internalError, tryLater, sigRequired, unauthorized, etc.);
3. a corresponding OCSP Response CERT payload is not received; OR
4. a [TBD] IKEv2 error is received indicating inability to respond.

4.2 OCSP Response

Upon receipt of an OCSP Responder Hash CERTREQ payload, the recipient SHALL either:

1. 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; OR
2. transmit a [TBD] IKEv2 error.

The recipient of an OCSP Responder Hash CERTREQ payload SHALL NOT ignore the request. At a minimum, a [TBD] IKEv2 error SHALL be sent.

An OCSP Response CERT payload SHALL be transmitted separate from any other CERT payload in an IKEv2 exchange.

Where multiple OCSP responses are useful to an environment, each such SHALL be transmitted via separate OCSP Response CERT payloads.

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 structure and encoding of the Certificate Data field of an OCSP Response CERT payload SHALL be identical to that 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 Baseline

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

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Responder</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) HDR, SAi1, KEi, Ni</td>
<td>--&gt;</td>
</tr>
<tr>
<td>(2)</td>
<td>&lt;-- HDR, SAr1, KEr, Nr,</td>
</tr>
<tr>
<td></td>
<td>CERTREQ(OCSP Responder Hash)</td>
</tr>
<tr>
<td>(3) HDR, SK {IDi, CERT(certificate)}, CERT(OCSP Response), CERTREQ(OCSP Responder Hash), [IDr,] AUTH, SAi2, TSi, TSr}</td>
<td>--&gt; HDR, SK {IDr, CERT(certificate), CERT(OCSP Response), AUTH, SAr2, TSi, TSr}</td>
</tr>
</tbody>
</table>

Figure 1: OCSP Extensions to Baseline IKEv2

In (2) Responder sends an OCSP Responder Hash CERTREQ payload identifying an OCSP responder trusted by 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 Responder Hash CERTREQ payload. In (4) Responder returns its certificate and a separate OCSP Response CERT payload covering that certificate.

It is important to note that in this scenario, Responder in (2) is not yet in possession of Initiator's certificate and therefore cannot form an OCSP request. However, [RFC2560] allows for pre-produced responses. It is thus easily inferred that OCSP responses can be produced in the absence of a corresponding request (OCSP nonces notwithstanding). In such instances OCSP Requests are simply index values into these data.

It is also important in extending IKEv2 towards OCSP in this scenario that Initiator have certain knowledge Responder is capable of and willing to participate in the extension. Yet 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. 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.
Figure 2: OCSP Extensions to EAP in IKEv2

In the EAP scenario, messages (5) through (8) are not relevant to this document. Note that while [IKEv2] allows for the optional inclusion of a CERTREQ in (2), this document asserts no need of its use. It is assumed that environments including this optional payload and yet wishing to implement the OCSP extension to IKEv2 are sufficiently robust as to accommodate this redundant payload.

6. Security Considerations

For the reasons noted above, OCSP Responder Hash is used in place of 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 Responder Hash does not contain such a nonce. But because the OCSP interaction is embedded in IKEv2, replay protection is nonetheless provided to the extent IKEv2 mitigates such attacks on its exchanges.

6. IANA Considerations

This document defines two new field types for use in the IKEv2 Cert Encoding field of the Certificate Payload format. Official values for "OCSP Responder Hash" and "OCSP Response" extensions to the Cert Encoding table of Section 3.6 of [IKEv2] need to be acquired from IANA.
7. References

7.1 Normative References


Authors’ Addresses

Michael Myers
TraceRoute Security LLC
EMail: mmyers@fastq.com

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bayern  81739
Germany
EMail: Hannes.Tschofenig@siemens.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

Myers & Tschofenig   draft-myers-ipsec-ikev2-oscp-01.txt   [Page 7]
The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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