OCSP over DNS

I-D Proposal by:
Massimiliano Pala (NYU)
Scott Rea (DigiCert)

OCSP over DNS

Table of Contents

Inconsistent Revocation

Industry Status Quo

- The CA attacks revealed that clients are inconsistent in handling revocation
  - Revocation information is not obtained in a timely manner
  - CRL validity lengths are often too long and lack fresh data due to caching
  - OCSP is not consistently deployed and used
  - Difficult to manage root and intermediate revocation

CAB Forum

Initiatives to Address Revocation

- CAB Forum is trying to address the deficiencies in revocation
  - Participants from ICAs, Browsers, Research & EDU, IETF, major Relying Parties
- Different problems from different perspectives
  - Revocation data availability problems
  - Access time to revocation services
  - High maintenance costs for high-volume environments
  - Managing trust anchor revocation
- Initial proposals
  - **Short term** → Lightweight OCSP Profile [RFC5019] + CDN friendly
  - **Mid term** → Smart fail revocation mechanisms in client software
  - **Long term** → Certificate issuance transparency and white lists

OCSP-over-DNS

The Background

- DNS can be used to distribute OCSP responses
  - No need for request/response protocol
  - Allows to lower the costs of distributing revInfo to clients
    - **Use of the DNS caching system**
  - Possible for SSL/TLS certificates for larger sites
- Current Challenges
  - OCSP responses waste bits on the wire if cert is valid
  - DNS allows for single UDP packet (if resp < 512bytes)
  - Use of EC keys might be advisable
  - Definition of DNS-based URLs for OCSP distribution
  - Allow for fallback URLs for backward compatibility
    - **Some clients only query the first URL in AIAs**

OCSP-over-DNS

The Objective

- The main goal is to enable a new OCSP response distribution mechanism using DNS
- OCSP-over-DNS approach allows clients to determine the status of digital certificates
  - specifically aimed at high-traffic secure Internet servers (i.e., SSL/TLS) by optimizing the delivery mechanism for revocation information distribution to the client.
- This transport protocol can be used in lieu of or in addition to other PKIX endorsed transport mechanisms such as HTTP.
- OCSP-over-DNS is meant to be used in conjunction with pre-computed OCSP responses.
- This document defines the DNS records to be used for OCSP data publication and the definition of additional URLs for the AuthorityInfoAccess (AIA) extension in certificates.

OCSP-over-DNS

Overview

- To validate a certificate using OCSP-over-DNS, the client should check the certificate for a DNS-based OCSP base URI, construct the URI for the specific certificate, and then retrieve the OCSP response from the DNS.
  - After this point, all procedures are to be performed according to the OCSP protocol as defined in [RFC5019].
- Steps:
  - 1. Lookup the OCSP URI provided in the AIA of the certificate to be checked. The format of the URI comprises the id-ad-ocsp identifier and a base URL where the scheme is dns://. The format of the full URI is discussed in the next section.
  - 2. Build the OCSP query for the certificate to be checked. This is done by pre-pending the hex representation of the digest of the certificate to the base domain provided in the OCSP DNS URI.
  - 3. Retrieve the DNS record carrying the required OCSP response. The Client SHOULD retrieve the revocation information directly through the DNS system. The distributed nature of DNS will allow for automatic load distribution.

OCSP-over-DNS

Defining DNS URLs in Certificates

- CAs provide the capability to check certificate status via OCSP by including the AuthorityInfoAccess extension in the certificate with an accessMethod of id-ad-ocsp and containing a URI in the accessLocation
  - This I-D defines an additional transport protocol (other than the standard HTTP defined in RFC 5280) – that of DNS
  - This transport mechanism is useful only in environments where OCSP responses are pre-computed
  - The accessLoaction SHOULD define 'dns' or 'dnssec' as the transport used to access the OCSP response data
  - Additionally the URL can optionally contain parameters to specify the digest algorithms to be used by clients to calculate the DNS query
    - Default is SHA256
- URL Definition follows
  - It has been brought to our attention that RFC 4501 already defines a DNS URI (analysis is required to evaluate our proposal against existing RFC)

OCSP-over-DNS

DNS URL Definition

- dnsurl = scheme COLON SLASH SLASH [base]

```
[QUESTION [ algorithm / oid]
; base: is the base hostname for
; the lookup operation.
; algorithm: is the text representation
; of the algorithm to be used to calculate
; the hash of the certificate

scheme = "dns" / "dnssec"

algorithm = "SHA1" / "SHA256" / "SHA384" / "SHA512"

oid = "OID" COLON oidvalue
; oidvalue is the string representation of
; the oid for the hash algorithm to be used
; to calculate the hash of the certificate

SLASH = %x2F ; forward slash ("/")
COLON = %x3A ; colon (":")
QUESTION = %x3F ; question mark ("?")
```

OCSP-over-DNS

DNS URL Definition

- The "dns" prefix indicates an entry or entries accessible from the configured DNS server. The "dnssec" prefix indicates, instead, an entry or entries accessible via the DNSSEC protocol and verification of the returned data SHOULD be performed.
  - Note that the <base> may contain literal IPv6 addresses as specified in Section 3.2.2 of [RFC3986].
- The <algorithm> construct is used to specify the digest algorithm that MUST be used to construct the final DNS query.
  - The allowable values are "SHA1", "SHA256", "SHA384", or "SHA512".
  - Alternative algorithms can be specified by use of OID
  - May need to expand this to allow for Hash parameters to be specified when relevant (e.g. GOST?)
  - E.g.
    - Using SHA1 = dns://somedomain?SHA1
    - Using MD5 = dns://somedomain?OID:1.2.840.113549.2.5
    - Using SHA256 = dns://somedomain

OCSP-over-DNS

Processing Steps

- Process steps for clients:
  - extract the <base> from the URL
  - pre-pend it with the hex representation of the digest value calculated over the DER representation of the certificate to be validated
  - the digest and the <base> values SHOULD be separated by the dot "." character.
  - the hash algorithm to be used is to be extracted from the AIA extension
  - if no value is specified, the SHA256 algorithm SHOULD be used to calculate the hash value
  - E.g. 4088439518ed222e9abf7555b954bd549b78325b.somedomain<base>

  - client queries the DNS for TXT records from the constructed query.
  - the returned value SHOULD contain the base64 encoded value of the OCSP response related to the certificate that needs to be validated.

Feedback

Invitation for Comments

- We invite feedback and additional collaborators on these ideas
  - See contact details on next slides
  - Including specific comments on the I-D

Contact Details

Relevant Links

Link to I-D:

https://datatracker.ietf.org/doc/draft-pala-rea-ocsp-over-dns/

Massimiliano Pala: pala@nyu.edu

Scott Rea: (801) 701-9636, Scott@DigiCert.com