Multiple OCSP Responses

In TLS Handshake

draft-pettersen-tls-ext-multiple-ocsp-01

Yngve N. Pettersen

Opera Software ASA

Problem statement

- The current status_request extension only allows OCSP for the site certificate
- Revocation information for intermediate CA certificate must be retrieved separately, causing delays and extra network traffic
- Using OCSP for intermediate CA certificates would give more timely information
- But OCSP for intermediates only useful if provided by TLS server, direct retrieval by client is too expensive for issuer

Proposal

- Issue: Current status_request extension cannot specify support for multiple formats, causing backward compatibility problems
- Solution: New extension status_request_v2 (provisional name)
- The new extension allows client to signal support for multiple response formats
- Old and new extension uses same CertificateStatus handshake message
- New response format is linked to Server's Certificate message sequence
- Benefits: Less client overhead, OCSP responder traffic predictable

New issue: Validity period of responses

With CertificateStatus the client depends on the server keeping the OCSP response up to date. But what if a server become a renegade and its certificate is revoked?

Until the server's OCSP response copy expires it can continue business.

- How to reduce window of opportunity for the renegade TLS server?
- Should clients ensure a short lifetime, bypassing server if it's too old?
- Should server-provided OCSP responses be requested and issued with a special extension, and with a short validity time?