Survey Results

Rick Andrews

6 March 2014, IETF 89 London

Summary

- 2 of 7 clients (Mozilla, Comodo) responded; some questions still unanswered from Mozilla
  - Promises from Microsoft and Google
- 1 of 15 servers (CloudFlare) responded
  - Promise from Microsoft; “no business advantage for us to respond so we will abstain” – Oracle
  - No response from Apache, reached out to OpenSSL: no time, worry about hidden agenda
- 20 of 67 OCSP responders responded

Server Survey (CloudFlare)

2b) Which cryptographic algorithms/parameters does the product support for the creation of keys and CSRs?

RSA 1024	DSA 1024	ECC nistp256	MD2	SHA1
RSA 2048	DSA 2048	ECC nistp384	MD4	SHA-256
RSA 3072	DSA 3072	ECC nistp521	MD5	SHA-384
RSA 4096	DSA 4096	ECC other		SHA-512
RSA other	DSA other			

Server Survey (CloudFlare)

8c) Does the product check staples before installing them? Yes

8d) How frequently are new staples fetched? Hourly

8e) What is the behavior of the server when it has no valid staple? “OCSP response: no response sent”

Client Survey (Mozilla)

11a) Which of the following status mechanisms does the product support? (check all that apply; if multiple mechanisms are used, please explain under which conditions they are each used)

1 - CRL - Firefox currently has very, very limited support for CRLs and will soon have none.

5 - AIA (where the location of the OCSP responder is obtained from the AIA extension)

6 - Stapled OCSP

7 - multiple-stapled OCSP (Not yet)

8 - CRL Sets (Not yet)

9 - Blacklists

11b) What order of priority amongst these mechanisms does the product follow? 9, 6, 5

Client Survey (Mozilla)

21) Which versions of SSL/TLS does the product support? SSL3, TLS 1.0, TLS 1.1, TLS 1.2

21) Does the product support SPDY? SPDY 3, 3.1

29d) Does the product ever offer cipher suites that are not supported in the TLS version advertised (i.e. AEAD cipher suites prior to TLS 1.2)? No, we aim not to, but see https://bugzilla.mozilla.org/show_bug.cgi?id=919677

Client Survey (Mozilla)

29a) Does the product support a ClientHello larger than 255 bytes? Yes

29h) Does the product support a ServerHello larger than 255 bytes? Yes

OCSP Responder Survey

Responses from Actalis, Autoridad de Certificacion Firmaprofesional, Buypass, Certinomis, Chunghwa Telecom Corporation, Comodo, Entrust, Government of Hong Kong (SAR)/Hongkong Post, HARICA, Izenpe S.A., KEYNECTIS, SwissSign AG, TeliaSonera, Trend Micro, TrustCenter, Trustis, VeriSign (Symantec), Axway, Safelayer Keyone, CloudFlare

OCSP Responder Survey

7 are CAs that write their own responder

11 are CAs that use third-party responders (or intend to)

2 are developers of third-party responder code

1 is a CDN, but uses nginx as proxy

OCSP Responder Survey

2) Does the product support RFC 5019, Lightweight OCSP? 3 Yes

3) Does the product support RFC 6960, OCSP Algorithm Agility? 2 Yes

4) What is the behavior if a request is made for a certificate serial number that had not been issued? 1 Revoked, 4 Unknown, 3 Unauthorized, 2 Good

Observations

Several people did not answer every question

Some client vendors asked for test sites

Apache responses are essential, but we've hit a roadblock

Testing might be more productive than reporting

Next Steps?

Extra slides

Server Survey (CloudFlare)

4b) Does the product validate the certificate path upon installation? Yes

4c) Does the product allow PKCS#7 import (in which the PKCS#7 file contains intermediates and end-entity certificates, and the product discerns which is which?) Yes

4f) Does the product ensure that the certificate chain is in the correct order? Yes

Server Survey (CloudFlare)

4g) Can the product be configured to send a self-signed certificate as part of the certificate chain when it is not the sole certificate? Yes

4h) Can the product be configured to send unrelated certificates in the certificate chain? No

5) Key/certificate renewal: Does the product require a restart in order to change its key pair? No

Server Survey (CloudFlare)

6) Which versions of SSL/TLS does the product support? SSL3, TLS 1.0, TLS 1.1, TLS 1.2

8a) Does the product support OCSP stapling in accordance with RFC 6066? Yes

8b) Does the product support OCSP multiple-stapling in accordance with RFC 6961? No