NIST Workshop: Improving Trust in the Online Marketplace

Revocation Process
Reasons for Revocation

• Security
  – Key Compromise
  – Malicious or fraudulent usage

• Business
  – Existing certificate replaced with a newer one
  – Subscriber no longer needs the certificate
  – Failure to uphold some portion of the Subscriber Agreement
Distribution of Certificate Status

• Certificate Revocation List (CRL)
  – RFC 5280
  – Digitally signed list of serial numbers of revoked certificates
  – Can contain reason for revocation and a revocation date for each serial number
  – URI in the CDP extension in certificates
  – Serial number listed = Revoked
  – Serial number NOT listed = Valid
Distribution of Certificate Status

• Online Certificate Status Protocol (OCSP)
  – RFCs 2560, 5019
  – Client requests status of one or more specific serial numbers
  – Server response is a digitally signed message stating ‘good’, ‘revoked’, or ‘unknown’, OR an unsigned error code.
  – URI to OCSP service in AIA extension
SCVP

• Server-Based Certificate Validation
  – RFC 5055
  – Client outsources path construction and/or validation to a trusted server
  – Not commonly used on the Internet
Revocation and Validation

CRL: http://example.com/ca.crl
OCSP: http://ocsp.example.com/
CRL Pros / Cons

• Con
  – Grow over time
    • 2007: 158KB
    • 2013: 41MB
  – Single list of “problematic” customers
  – No positive confirmation
• Pro
  – Potentially more efficient for CAs that issue very few certs that are unlikely to be revoked.
OCSP Pros / Cons

• Pro
  – Small, constant size
  – Can provide real-time status
  – Can provide positive confirmation
    • CA/Browser Forum Baseline Requirements: 8/1/2013

• Con
  – Requires a request/response cycle for each certificate encountered by a client
    • Adds latency to TLS handshake
    • Significant load on OCSP service
Criticisms

• Performance impact
  – https://revocation-report.x509labs.com/

• Privacy

• Client not always able to obtain status
  – Captive portals
  – Egress filtering
  – Random network failures

• “It only works when you don’t need it.”
OCSP Stapling

- RFC 6066 (Certificate Status extension)
- Server retrieves and caches OCSP response for its certificate
- Server provides OCSP response to client in TLS handshake
OCSP Stapling

OCSP: http://ocsp.example.com/

Certificate Authority
- CRLs (Web Server)
- OCSP

SSL Customer
- Web Server

User
- Mozilla Firefox
- Internet Explorer
OCSP Stapling

• Performance Impact
  – No separate connection to OCSP service
  – However, potentially adds additional round trips

• Privacy
  – CA only receives requests from its customers

• Client not always able to obtain Status
  – Client receives OCSP response from the web server

• “It only works when you don’t need it”
  – Attacker has to block web server from getting updated OCSP response
OCSP Stapling: Issues

• Performance
  – Overflow initial congestion window

• Limited to single OCSP response

• Server support
  – IIS 7, Apache httpd 2.4+, nginx 1.3.7+

• Client support
  – Varies based on platform/library/toolkit
No-Fail vs. Soft-Fail vs. Hard-Fail

• No-Fail: Don’t even check for revocation
• Soft-Fail: Client allows TLS handshake to proceed if unable to determine certificate status
• Hard-Fail: Client allows TLS handshake to proceed IFF it can determine the certificate is still valid
Why not Hard-Fail?

• Client priorities and competition
  – Performance
  – “Show the page”

• Potentially creates new DoS vector

• Transition to OCSP Stapling
  – “Must-Staple” extension
Varied Levels of Support

• Clients have differing behaviors
  – Different versions of the same client
  – Same client running on different platforms

• Behavior may depend on version of underlying library/toolkit

• Some clients have implemented their own solutions

• Many non-browser clients do no revocation checking at all
Recommendations

• OCSP Stapling (multiple certificate status)
• CAs should avoid delegated OCSP signing
• Libraries/Toolkits should provide high-level APIs for applications
• Better education/awareness