Certificate Revocation With OCSP

Keith Bogart

CCIE #4923

- kbogart@ine.com
- @keithbogart1
- linkedin.com/in/keith-bogart-2a75042

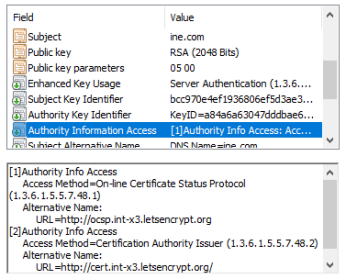
CCIE Routing & Switching

Topic Overview

- OCSP Definition & Functionality
- OCSP Browser Support
- OCSP Stapling
- OCSP Must-Staple

OCSP

- Online Certificate Status Protocol
- Web Client submits a request to a CA server, that returns a signed response with certificate current status.
- Problem areas;
  - OCSP Query between client and CA servers during TLS handshake increases latency.
  - Relies on CA infrastructure making it prone to availability problems.
  - Privacy compromise. Browser leaks what website is being accessed and who accesses it to CA servers.
  - Tremendous load on CA Servers to respond to gazillions of OCSP Requests.



To use OCSP, the CA must encode the OCSP server location into the certificates that it signs. The “Authority Information Access” extension is used for this.

-

OCSP requests contains the Serial number of the Certificate in question.

-

Notice that OCSP Response is “signed” by the CA. This prevents anyone else from spoofing the CA and spoofing an OCSP Response.

-

CA Servers are a ripe target for malicious actors to attack because they are known, public sources of critical data.

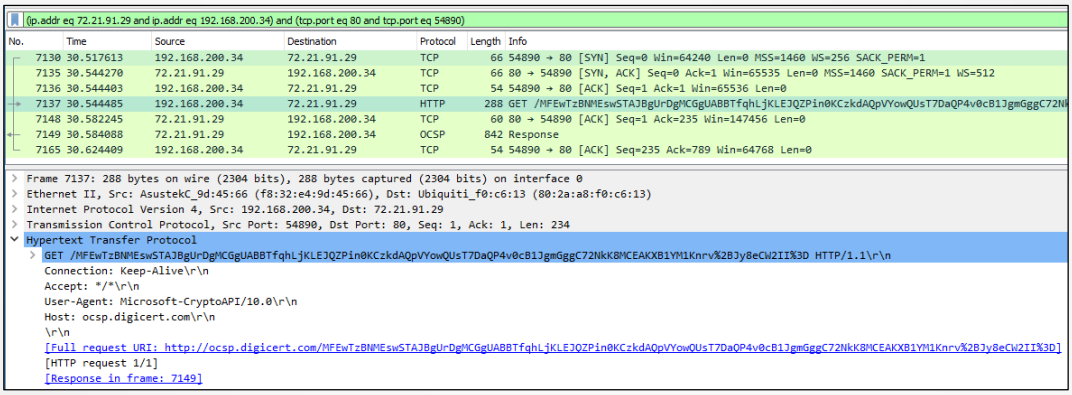
-

OCSP does not mandate encryption, everything is sent in cleartext. When an OCSP Request is sent:
----The CA knows that a specific website Certificate was just viewed and your IP address

OCSP Browser Support

- OCSP is supported by the following Web Browsers:
  - Internet Explorer (starting in Windows Vista)
  - All versions of Mozilla Firefox (on by default in Firefox 3 and later)
  - Safari on MacOS (on by default as of Mac OS X 10.7)
  - Opera starting with version 8.0
  - Microsoft Edge
- OCSP Soft Fail
  - Failure to receive OCSP Response doesn't mean Certificate is invalid…just that CA is unreachable/unresponsive.
  - Most browsers simply treat the Certificate as valid in this case…this is called, "Soft Fail"
- Google Chrome does not support OCSP but instead implements its own revocation-checking mechanism.

OCSP Capture



OCSP Stapling

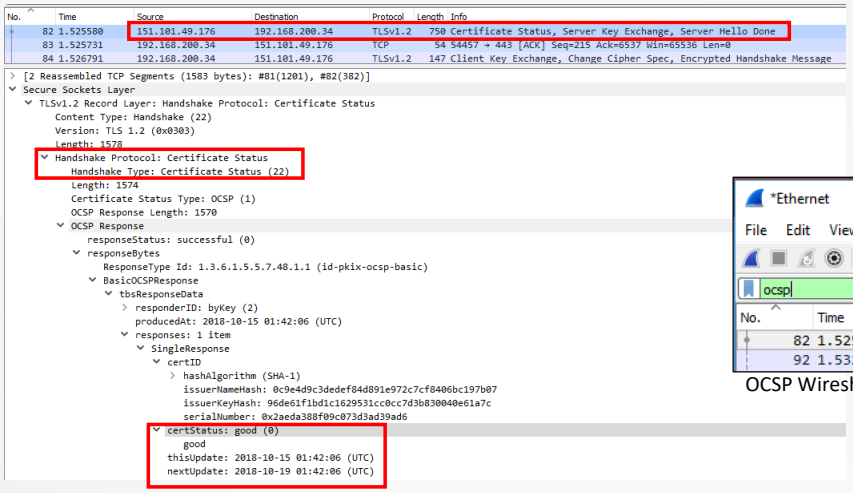
- Normal OCSP protocol requires Web Client to directly query the Certificate Authority (using OCSP) for status of website Certificate.
- OCSP Stapling moves this responsibility to the Web Server itself.
  - Web Server will periodically poll CA (via OCSP) for revocation status of its own Certificate.
  - Web Server will "staple" this OCSP Response along with certificate to the client during TLS handshake in a "ServerCertificateStatus" message.
  - In this way, the CA will not know when a Client is visiting any particular website.
- Downsides: OCSP-Stapling is not mandatory, and clients don't know when to expect it.
  - When Cert is received without an OCSP Staple, web-client proceeds to using normal OCSP (if anything at all) to verify revocation status.

OCSP Stapling would be great if EVERY website did it. Then, browsers could be programmed that if they connected to a website, downloaded its Cert and there WASN'T a staple…game over! That site must be a fake!

-

Most websites that utilize HTTPS also implement OCSP Stapling.

OCSP Staple Capture



OCSP Wireshark Filter

How can you tell that this is an OCSP-Staple (as opposed to a normal OCSP transaction between a Client and a CA)?? Two indicators:

----OCSP is sent using HTTP…not HTTPS (so it wouldn't show up in Wireshark as TLS)

----Take a look at the IP Source Address of the "Certificate Status" message. It is the same source IP as the website itself.

OCSP Must-Staple

- OCSP-Stapling is not mandatory, and clients don't know when to expect it.
- OCSP Must-Staple is an extension to a Digital Certificate
  - Must be requested in CSR (Certificate Signing Request)
  - Certificate Authority will append OCSP Must-Staple to Certificate
  - Added as X.509v3 Extension
- When Server Certificate is presented to Web Client, presence of this extension indicates (to the Client) that the Cert is ONLY valid if an OCSP Status Response immediately follows.
- More details: RFC 7633

In this way, even if someone did steal the private key and Certificate of a website…and even IF they did manage to convince you to navigate to their spoofed website…the moment you received a copy of the Cert you would wait (for a few milliseconds) for an OCSP Response…which of course they couldn't give you. And then your browser would block this website and declare it to be unsafe.

-

OCSP Responses are digitally signed by the CA with the CA's private key and contain the Serial number of the Cert. There is no way to spoof them. And if a Malicious Actor tries to remove this extension from a Cert…then the Signature of that Cert will no longer be valid.

OCSP Must-Staple