Guide to OCSP Stapling

THAWTE TECHNICAL REPORT

Guide to OCSP Stapling

This report explains Online Certificate Status Protocol (OCSP) Stapling, a technology that speeds the delivery of certificate status information to your web site's users. Use this report to determine if OCSP Stapling is right for you and your website.

Introduction

When a browser user visits a web site that provides an SSL or TLS[1] certificate, the browser performs a number of checks to verify that the web site's certificate is valid. One of those checks is a certificate status check to see if the certificate is still valid, or if it has been revoked. Certificates can be revoked for a variety of reasons, but by and large the browser just wants to know if the certificate is valid. This is generally done by one of two methods:

- Certificate Revocation List (CRL), a list of serial numbers of all revoked certificates that were issued by a particular CA certificate. The entire CRL is signed by the Certificate Authority (CA) so the browser can be assured that it's authentic and hasn't been tampered with.

- Online Certificate Status Protocol (OCSP), in which a request is made for a specific SSL certificate and a response is returned that indicates whether that certificate is valid or revoked. The OCSP response is signed by the CA so the browser can be assured that it's authentic and hasn't been tampered with. OCSP is defined in IETF RFC 2560 and RFC 5019.

Although they provide similar information, CRLs are not related to OCSP and won't be discussed further in this report. Most modern browsers rely on OCSP instead of CRLs.

Traditionally, a browser would get the OCSP response from the CA, since the CA knows the current status of the certificate and is able to digitally sign the response. However, in an effort to improve the speed and reliability of OCSP, a new model was developed in which the web site gets the OCSP response from the CA and sends the OCSP response to the browser in the SSL handshake. This can be more efficient because the OCSP response is valid for hours or days, and the web site can cache it and send it to all users during that time period. Also, this model eliminates the need for the browser to initiate a connection to the CA, thereby saving time.

The first version of OCSP Stapling was defined in an IETF RFC, although you won't see the word "stapling" in that document – it's called "status_request" instead. The idea is that during the initial SSL handshake when the web site sends its SSL certificate to the browser, it can also attach or "staple" its OCSP response. At the cost of some extra bytes in the handshake between client and server, OCSP stapling spares the client from having to initiate a separate connection to the CA and wait for the response.

Advantages

The obvious advantage to OCSP Stapling is the improvement in speed and availability of the OCSP certificate status check.

Some have stated that OCSP Stapling helps maintain the privacy of the end user, since a CA can see which web sites a user has visited (only those web sites that have certificates issued by the CA). If OCSP Stapling is used, the CA will see OCSP requests only from the web site, not the web site's end users.

Many wi-fi hotspots use Captive Portals to control access to the Internet, sometimes requiring entry of a credit card number to pay for access. In such environments, users are not able to check the status of the SSL certificate used by the Captive Portal, since all Internet access is blocked until authentication and/or payment is successful. If the Captive Portal used OCSP Stapling, it could allow its users to see and verify its SSL certificate status before those users proceed.

Also, Microsoft's Internet Information Services (IIS) web server has supported OCSP Stapling for some time (since version IIS 7), and it is enabled by default.

1. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are often used interchangeably. In this document, SSL will be used. The reader will understand that everything applies to TLS as well.

Disadvantages

There are several disadvantages of OCSP Stapling to be aware of:

Support for OCSP Stapling is not yet widespread among typical modern browsers. Both browser and web server must support OCSP Stapling. If either endpoint does not support it, the browser will have to contact the CA to get a CRL or OCSP response.

Nearly all SSL certificates today are signed by an intermediate CA certificate, which is itself signed by a root certificate. Web servers with such certificates typically send the client its own certificate and the intermediate CA certificate. But browsers need to check the status of both certificates, since either one could have been revoked. Unfortunately, the specification of OCSP Stapling allows for only one certificate status to be sent in the SSL handshake. There's a revised version of the specification that defines "multi-level stapling", or the ability for the web server to send the client OCSP responses for multiple certificates. Deployment of multi-level stapling will lag behind the deployment of single-level stapling.

Support for OCSP Stapling has recently appeared in web servers such as Apache HTTP Server (version 2.3.3, if using OpenSSL 0.9.8h or later) and nginx (version 1.3.7). If you use those servers, you may need to upgrade them to a recent version to take advantage of OCSP Stapling. If you don't use those servers or Microsoft IIS, you'll need to check with your web server vendor to see if OCSP Stapling support is available. Upgrading or changing your web server software is potentially risky, and should only be done when you're able to fully test the new software.

Your web server will need to be able to communicate with the CA periodically in order to get an updated OCSP response. Your company's security policy may need to be modified to allow that. Typically, web servers accept incoming connections from the Internet but don't initiate any outgoing connections. OCSP Stapling requires the web server to periodically (perhaps once per day) initiate an outgoing connection.

What is Thawte doing about OCSP Stapling?

Thawte helps customers maintain high security for their web sites. You don't need a special SSL certificate to take advantage of OCSP Stapling. In fact, you don't need Thawte's involvement at all. Thawte's infrastructure for serving OCSP responses will respond to any requester, whether it's the client browser or the web server. At this time, Thawte's own web sites don't support OCSP Stapling.

Details

If you would try out OCSP Stapling, here's what to do:

Check your web server software, and change or upgrade if necessary to get OCSP Stapling support. Check that your company's security policy and firewall rules allow your web server to communicate over the Internet to the CA.

If you're web site is hosted by a hosting company or is fronted by a Content Delivery Network (CDN), you'll need to check with your hosting company or CDN provider to see if they can support OCSP Stapling.

Finally, if you try OCSP Stapling but decide it's not advantageous, you can simply disable the feature on your web server.

Conclusion

OCSP Stapling may be advantageous to web site owners who wish to improve the performance of their end users as they access the site. Although it has some shortcomings, it might make a difference for some web sites, especially those with high numbers of users.

UID 207/11/13