The Online Certificate Status Protocol (OCSP) allows for real-time verification of a certificate's validity. How does OCSP improve upon traditional methods like Certificate Revocation Lists (CRLs) and are there any privacy concerns associated with its use?

Answer: There are several things that OCSP improves upon, like Real time verification, efficiency, and timeliness. The privacy concerns vary and cover the following: Privacy leakage, Dependency on CA and OCSP stapling.

OCSP stapling, or the TLS Certificate Status Request extension, is seen as an improvement over standard OCSP. How does OCSP stapling work, and why is it considered more efficient and privacy-preserving than traditional OCSP?

Answer: OCSP stapling aims to reduce latency by improving efficiency. Then enhances privacy by minimizing direct client queries to the OCSP responders. This puts more control in the hands of the server and provides an effective means of certificate revocation check during the TLS handshake.

In the event a certificate needs to be revoked, how does the OCSP handle this? How quickly can a potentially compromised certificate be flagged as invalid, protecting users from malicious sites?

Answer: OCSP has real time validation of certificate status. This allows potentially compromised certificates to be quickly flagged as invalid during the TLS handshake. If that happens, users are prohibited from accessing the sites with compromised certificates.