PKI (part 2) summary

zondag 8 januari 2023 11:25

Revocation - CRL

CRLs are signed lists of revoked certificates. They contain the time at which they were produced, as well as the time at which the CRL will next be updated. One major problem is that they grow very large, and will usually produce high load at the update time.

Types of CRLs

- Over-Issued CRL: issue CRLs more often than only at the nextUpdate time. Provides better load distribution.
- Delta CRL: contains changes since a base CRL was issued. Provides smaller CRLs.
- Indirect CRL: the issuer of the CRL is not equal to the certificate issuer. Allows different security levels for CRL and certificate signing.
- Segmented CRL: separate revocation information into multiple CRLs.
- Redirect CRL: CRL which points to actual CRL. Easier to distribute.

Revocation - OCSP

OCSP allows clients to request the status of one or multiple certificates by querying a responder. Responses are signed, and can include:

- Unknown (nothing known about the certificate)
- Revoked
- Good (certificate not revoked, or expired, or does not exist)

Signed responses can be stored an provided as a proof of validity in the nearby future (OCSP stapling).

Revocation - Novomodo

In certificate, include $H(R)$ and $H^{365}(T)$. On day i, publish R if the certificate was revoked, or $H^{i}(T)$ if the certificate is still valid. The certificate only needs to contain two additional hash values, while the status information consists of a single hash value.

Certificate Transparency

Only consider certificates to be valid if they are included in a (blockchain-like) public log. This makes it (nearly) impossible for CAs to secretly issue valid certificates.