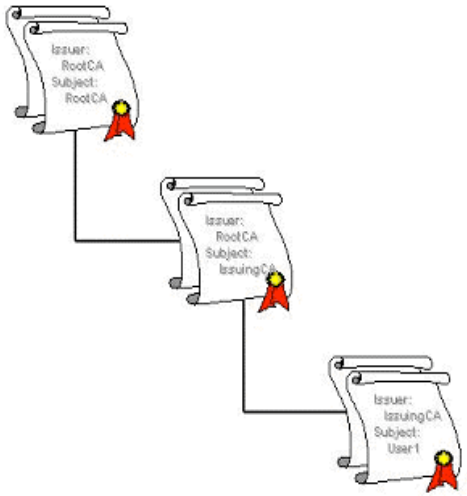
Making X.509 Certificate Revocation Robust

Magnus Nyström, Microsoft
Rangan Doreswamy, VeriSign

Current Approach



- Revocation check is top-down
  - Establish revocation status of CA cert using CDP or AIA first
  - Then establish revocation status of end-entity certificate

- Revocation information comes from the subject certificate, not the issuer
- Serial number of the certificate used as identifier (together with issuer name)

Limitations

- Revocation checks not effective in case of hash collision attacks
  - Attacker has full control over “rogue” certificate
  - CDP or AIA in the certificate can be spoofed or excluded completely
  - Issuing CA cannot revoke the rogue certificate
- Serial number not a strong enough identifier
  - Attacker may or may not change the serial number for the rogue certificate

Proposal

- 2 new extensions in the issuer certificate
  - Issued Certificate Revocation List Distribution Point (ICRLDP): A pointer to revocation data for all issued certificates.
  - Similarly, a new OCSP AIA extension for OCSP for all issued certificates
- New certificate identification for revocation check
  - Full certificate hash instead of CertificateSerialNumber
    - Changes the CRL entry for the new ICRLDP extension
    - Changes the OCSP request for the new OCSP AIA extension in issuer certificate

Considerations

- New extensions take precedence; but are optional
  - No changes to current CDP/AIA extensions
  - If new extensions are absent, existing revocation check mechanism continues to be used as a fallback
- No changes for end-entity certificates
  - Corollary benefit: Update revocation endpoints without re-issuing end-entity certificates
- Requires changes in CA issuance and path validation
  - Update the issuing CA and root CA certificates
  - Revocation endpoints specified by a CA 2-levels up in hierarchy

Summary & Next Steps

- Desirable to build resiliency against weaknesses in cryptographic hash algorithms
- Expected to be a long term change
  - E.g. when renewing roots or creating new roots
- Proposed next step:
  - Initiate work on a Internet-Draft describing the proposal in further detail

Discussion?