Certificate Limitation Profile

Application-level trust amendments

Dmitry Belyavskiy

Technical Centre of Internet/Cryptocom.ru

IETF 103, Bangkok

Certificate trust: PKI

- Binary model of trust
  - Trusted CAs
  - CRL/OCSP
  - CA-driven revocation

Google vs Symantec (2017)

- “Too big to fail” CA
- List of limitations:
  - A reduction in the accepted validity period.
  - An incremental distrust of all currently-trusted Symantec-issued certificates.
  - Removal of recognition of the Extended Validation status of Symantec issued certificates.

Source: https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/eUAKwjihhBs/rpxMXjZHCQAJ

Application-level trust now

- Managing list of trusted CAs
- CRL/OCSP validation
  - What if OCSP is unavailable?
- Hardcode in case of limitations

Proposed solution: CLP

- List distributed with/by application
- CRL-like syntax, crypto-signed format
- Shared codebase instead of app-level hardcode

https://datatracker.ietf.org/doc/draft-belyavskiy-certificate-limitation-policy/

List of limitation

- **maxIssued** – no trust to certs issued after
- **maxValidity** – no trust to certs after
- **validityPeriod** – maximum validity period
- **ignored/required X509Extensions**
- **Name constraints**
- **requiredNativeChecking** – apply CA native CRL/OCSP, fail if not available
- **forbidIntermediate**

Some details

- Limitations applied to: **Itself/descendants**
- CLP verification:
  - Special Key Usage of Signer key
  - Check matching to internal requirements
  - No reason to allow unsigned CLPs
- Application-level checks
  - CLP in use
  - Minimal date of issuance
  - Signed by correct trust anchor

Verification process with CLP

- Build chain of trust
- Process from root till the end
- Apply limitations to the matching certs

Current approaches

- Browsers: internal implementations
  - At least Chrome and Mozilla
- P11-glue

Questions?

beldmit@gmail.com