CA Perspective on Web PKI

Ben Wilson - DigiCert

Background

- Web PKI has been evolving for 15+ years
- Web PKI environment is global and open (www=wild, wild west) – "Neither CAs nor browsers have market incentives to compete on the basis of security."
- Many legacy and new implementations do not conform to the RFCs promulgated by PKIX.
- A survey of PKI on the web will inform us on functionalities and an evolution strategy.

Scope

- Practical, real-world observations and implications re: the behavior of clients, servers, proxies, etc.
- Not the user interface (area for W3C or browsers)
- Mobile devices and apps included in scope
- Problems identified with certificate processing

  (i.e., there is a natural tendency toward disorder and chaos, with its resulting corollary-“if anything can go wrong, it will.”)

Behaviors to Survey

- Criticality of Name Constraints Extension (Mozilla new subCA Policy vs. Apple's implementation)
- Effects of revocation on access to content ("upon transmission or receipt of a fatal alert message, both parties immediately close the connection")
- CRL-fed OCSP responses vs. direct OCSP (RFC 2560 discussion of "good" responses)
- RFC 2818 (2000) – use of CNs deprecated in favor of SANs (but what devices choke on certs w/o CNs?)

Behaviors to Survey (cont)

- RFC 5280 dNSName processing
- RFC 5280 certificate chain variables (name encoding, policy OIDs, superfluous certs, signature algorithms, revocation checking methods, AIA chasing, etc.)
- Cache/store behaviors (CRLs, OCSP, roots, chains, etc.)
- OCSP GET vs. POST and Nonce (CDN-friendly)
- Key strength and algorithm support (SHA256, etc.)
- OCSP Stapling support

Goals

- Identify the current landscape and document the relevant maturity model
- Develop a roadmap to address legacy systems, pinpoint status of adoption and progression
- Guide the evolution and migration of WebPKI
- Provide guidance for developers for present use and to plan for future developments
- Encourage the harmonization of behaviors