Field and extension processing for Certificates, CRLs, and OCSP

Jeremy Rowley

DigiCert, Inc.

Overview

- Certificate fields and extensions
  - Potential conditions are numerous
  - Surprising behavior by user agents
  - Different reaction offline v. online
- Consistent behavior is important
  - Different behavior causes confusion
  - RFC v. real world implementations (e.g. Firefox extended key usage and non-critical name constraints)
  - Performance and security issue
  - Documented reasons for different behavior
- Frame new Internet Drafts and possibly update inconsistent/confusing Internet Drafts

Limiting the Scope

- Too many variables
- 6 User Agents with varying versions
  - Chrome, Safari for OSX, Safari for Windows, Firefox, IE, Opera
- 30 Operating Systems / Platforms
  - Includes 10 mobile devices and apps
  - OSX, Windows XP, Windows Vista, Windows 7, Windows 8, Ubunto, Android, iOS, Wii, DS, Brew…
- 300 conditions
  - Name mismatch, expired, before validity period, CRL…

Current Status

Tabbed Spreadsheet on Google Drive

Three types of sheets

Reference Sheets:

- Conditions (name mismatch, expired, revoked)
- UA Behaviors (visual cues and bypassable errors)
- Sets the limits on scope

Input sheets for User Agents, OSs, & Platforms
(Safari on Win7, Firefox on Android, Opera on Wii)

Results sheets for summary of conditions

Tasks

- Complete “Conditions” List
- Identify key platform and OS versions
- Identify key user agents
- Eliminate where user agents not on OS/platform
- Complete survey
- Fill in the gaps with tests

Next Steps

- Identify and summarize current landscape
  - Crowd-sourcing with open access to spreadsheets
  - Q2 completion goal
- Use information to evolve WebPKI
  - Create field and extension document (Feb 2014)
  - Identify common deviations and resulting abnormalities
  - Road map for legacy systems
  - Provide guidance for developers for present use and to plan for future developments
- Field and extension document will encourage harmonization of behaviors and help restrict use of conflicting extensions