RPKI Validator Interoperability Testing

Participants: R. Austein,
T. Bruijnzeels, A. Chi

Interop Testing, Mon 3/28/11

- Goal: informally verify that three validators give same results on basic repository data.
  - rcynic validator (C, OpenSSL)
  - RIPE NCC validator (Java, BouncyCastle ASN.1)
  - BBN validator (C, OpenSSL, Cryptlib, BBN ASN.1)
- Method: compare each validator's list of "fully validated" objects when run against each of 5 repositories.
  - BBN test repo, RIPE, APNIC, LACNIC, AFRINIC. Repos had no intentional misbehavior.

Validator Comparison

	Rcynic validator	RIPE NCC validator	BBN validator
RIPE NCC repo (w/ known UTF8String issue)	Full acceptance	Full acceptance	Full acceptance (if permitting UTF8String)
APNIC repo	Partial acceptance (reject some expired objects) *Matches RIPE validator*	Partial acceptance (reject some expired objects) *Matches rcynic validator*	Analysis incomplete, due to validator bug and rejection of T61String
AFRINIC repo	Full acceptance	Full acceptance	Full acceptance
LACNIC repo (w/ known keyUsage issue)	Full acceptance	Mostly reject due to missing keyUsage	Mostly reject due to missing keyUsage
BBN repo (w/ probable rsync server issues)	Full acceptance	Full acceptance	Full acceptance

Results

- Bugs were identified for rcynic and BBN validators.
- Minor bugs were identified for repositories.
- Discussion between participants revealed differences:
  - If a directory contains a valid signed certificate that is not listed on the manifest, rcynic and RIPE validator ignore the certificate. BBN accepts the certificate but flags it. Randy Bush thinks the latter is correct.
  - Handling of stale CRLs and manifests currently varies across implementations.
- Overall, all participants deemed the interop testing a useful exercise. Future interop testing should occur when new functionality has been added (e.g. ghostbusters, RTR). In addition, it should test responses to misbehavior.
- Other validators welcome!