NIST Path Discovery Test Suite

David Cooper
May 25, 2005

Talk Outline

- Overview of plans for path discovery test suite
- Current Status and development plans
- Description of initial draft of test suite

Overview of test suite

- Test suite will consist of a set of PKIs
- PKIs will differ in:
  - Complexity of architecture: hierarchy, simple mesh, complex mesh
  - Mechanisms available to locate certificates and CRLs.
- Tests will be developed for four levels of complexity: Rudimentary, Basic, Intermediate, and Advanced.

Rudimentary

- Intra-organizational applications
- Architecture: Hierarchical (but trust anchor CA has issued peer-to-peer cross-certificates)
- No constraints in paths to be constructed
- Self-issued certificates
- Certificates and CRLs signed with different keys

Basic

- Complexity comparable to current Federal PKI architecture
- Mesh architecture with only one path from any CA to any other CA (although two certificates issued by “Common Policy Root CA” to “FBCA”)
- Name constraints
- Policy mappings
- Policy constraints

Intermediate

- Mesh architecture with multiple cross-certified bridge CAs.
- Multiple paths between CAs.
- Constraints may result in one path being valid and another being invalid
  - There may be a path to CA X through Bridge A and through Bridge B, but only one path is valid.

Advanced

- TBD. Some features of Advanced architecture may include
  - Missing and mismatched key identifiers
  - More complicated key rollover tests
  - CAs that use different keys to sign certificates and CRLs
  - AIA/SIA extensions in which information is spread across multiple access locations

Location Techniques

- Directory based – locate certificates and CRLs based on DNs in **issuer** and **subject** fields and **cRLDistributionPoints** extension.
- LDAP URI based – locate certificates and CRLs based on LDAP URIs in **authorityInfoAccess**, **subjectInfoAccess**, and **cRLDistributionPoints** extensions.
- HTTP URI based – locate certificates and CRLs based on HTTP URIs in **authorityInfoAccess**, **subjectInfoAccess**, and **cRLDistributionPoints** extensions.

Current Status and Future Plans

- Initial drafts of Rudimentary and Basic levels will be made available soon.
- Comments on initial draft due by July 1, 2005
- Comments will be used to modify Basic and Rudimentary levels and as input to development of Intermediate level.
- Draft Intermediate level tests will be made available for review and comment prior to development of Advanced level.

Overview of Current Tests

- Current test suite includes three distinct PKIs.
- The three PKIs are almost identical to each other with the exception of the methods used to indicate where certificates and CRLs are located:
  1. Directory based: Location implicit in DNs in issuer, subject, and CDP.
  2. LDAP: LDAP URIs included in AIA, SIA, and CDP extensions.
  3. HTTP: HTTP URIs included in AIA, SIA, and CDP extensions.

Rudimentary Level Tests

- All certificates needed for validation are hierarchically subordinate to trust anchor.
- Certification paths can be validated using an Enterprise Path Validation Module (PVM)[1]
- Includes certification paths that mimic the effects of key rollover.
- Includes ARLs and CRLs, some stored in CAs directory entry and some stored in distribution points.

[1]See NIST Recommendation for X.509 Path Validation

Basic Level Tests

- Mesh Architecture, portions of which mimic the current Federal PKI.
- Certification paths can be validated using an Enterprise Path Validation Module (PVM) that can also process policyMappings, policyConstraints, anyPolicy OID, and nameConstraints (DN only).

Running the Tests

- Intermediate certificates and CRLs will be made available on NIST LDAP and HTTP servers.
- Test descriptions, trust Anchor (self-signed) certificates, and end entity certificates will be posted on NIST Web server.
- Information will be available at

  http://csrc.nist.gov/pki/testing/pathdiscovery.html

Questions