Developer Workshop

Charles Schmidt – The MITRE Corp.

September 28, 2010

MITRE

Supported by NSA contract number W15P7T-10-C-F600

Topics

- Unique Benchmark IDs
- Local vs. Remote Imports
- XCCDF-to-XCCDF references
- XCCDF 2.0 kickoff

- There will be a break at 11:15, corresponding with the normal section breaks

Supported by NSA contract number W15P7T-10-C-F600

Unique Benchmark IDs

- Benchmark id properties are supposed to be globally unique
  - Should identify a specific version of a specific document
- Currently there are no conventions that help support this
  - Examples of id collisions have been observed
- How do we better prevent id collisions?
  - Enforce conventions via schema? (Major change)
  - How do we enforce uniqueness?
    - E.g., fields with namespaces, etc.
  - What about other IDs (Rules, Groups, etc.)

Supported by NSA contract number W15P7T-10-C-F600

Unique Benchmark IDs – Sample Proposal

- Adopt convention of fields within the id
  - xccdf:usgcb.nist.gov:1.0.0.0:WindowsXP
    - Requires changing the id type from NCName to a string
    - Follows the conventions of other standards (OVAL, OCIL)
  - Write conventions into specification now; enforce in schema in XCCDF 2.0

Supported by NSA contract number W15P7T-10-C-F600

Local vs. Remote Imports

- XCCDF references 6 imported schemas
  - XML Namespaces, Dublin Core, CIS Platform Schema (deprecated), XCCDF-P (deprecated), CPE 1.0 (deprecated), CPE 2.3
- All imports assume schema file is local and in same directory as XCCDF
- Proposals made to have imports point to canonical remote documents
  - Change schemaLocation attribute:
    - From: simpledc20021212.xsd
    - To: http://dublincore.org/schemas/xmls/simpledc20021212.xsd
- Previous discussion led to deadlock

Supported by NSA contract number W15P7T-10-C-F600

Local vs. Remote Imports – Previous Arguments

- Remote references
  - Always pointing to latest version (if site supports)
  - Eliminates branching of standards suites
    - E.g. XCCDF points to CPE 2.3, but OVAL points to CPE 2.2
    - Is branching already written into the XCCDF specification?
  - Named source is always correct
- Local references
  - Do not require remote access
    - Tools could intercept remote references and load locally
      - But doesn't this obviate the advantages of remote references
  - Give tools and users direct control over which schemas to import
    - Without modifying XCCDF schema or implementing intercepts

Supported by NSA contract number W15P7T-10-C-F600

XCCDF-to-XCCDF References

- Allow XCCDF documents to directly use external XCCDF content
  - Possibly call another whole benchmark as part of a check
- Previous discussions were favorable, but suggested deferral
- Major challenges are XCCDF processing and tailoring
  - How much of document processing should a limited reference require?
  - How would tailoring information (beyond individual Value values) be transferred?
- Change also complicates tools – XCCDF interpreters might now be in the middle of the call stack instead of the top

Supported by NSA contract number W15P7T-10-C-F600

XCCDF-to-XCCDF References – Sample Proposal

- <check-export> element in checks
  - Holds an XML structure defined by the target language
  - In XCCDF, this structure could be a Profile, selecting tailoring options in the target document
- This still doesn't answer questions of document processing and efficiency
- The above proposal is effectively an "external Profile", as discussed in previous meetings
  - Community decided not to support external Profiles, but several members have requested a review of this decision

Supported by NSA contract number W15P7T-10-C-F600

XCCDF 2.0

- Major change
  - Backward content compatibility not necessarily preserved
- Main question: is there a need for a change of this scale
- If the floodgates are opened, what do we want the outcome to be
  - Within reason, if a major change is going to be endured by content producers and vendors, we should make changes to address far-reaching issues to push back the next major change

Supported by NSA contract number W15P7T-10-C-F600

XCCDF 2.0 Possible Modifications – Use Cases

- XCCDF names 7 (overlapping) use cases
- My summary (paraphrasing and merging)
  - Express guidance
    - Configuration policy
    - Vulnerability alerts
  - Support conversion to other formats
    - Human readable
    - Structured content
  - Enable tools to perform automated assessments of systems
    - Report on findings
  - Support remediation based on assessment findings
  - Support tailoring by auditors and system administrators

Supported by NSA contract number W15P7T-10-C-F600

XCCDF 2.0 Possible Modifications – Use Cases - Questions

- XCCDF still has little uptake for vulnerability reporting
  - CVRF created to meet perceived gaps
  - Modify XCCDF to better fit? Drop use case?
- Automated assessment works well when target is a single device
  - Users have proposed using XCCDF for multi-role policies
    - User+devices; multiple devices in different roles
  - XCCDF doesn't have good mechanisms to treat multiple targets differently
- XCCDF results are a data dump – some have requested logic to allow targeted reporting

Supported by NSA contract number W15P7T-10-C-F600

XCCDF 2.0 Possible Modifications – Specification Structure

- Split specification into multiple documents
  - Similar to CPE 2.3
- Could split by use case
  - Automation control; guidance encapsulation; vulnerability description; remediation; etc.
  - Vendors could focus on compositions of sub-specification rather than picking from the whole
  - Might require schema re-organization
- Could split by document usage
  - Structure and content vs. document processing
  - Might simplify reading

Supported by NSA contract number W15P7T-10-C-F600

XCCDF 2.0 – Final Considerations

- **XCCDF 2.0 is not necessarily imminent**
  - **Requires a strong community desire for capabilities that are only possible in a major release**
  - **If changes can be made in backward compatible ways, we will do so**
- **If a major release occurs, this is the best time to submit proposals for how you wish XCCDF could be used**

Supported by NSA contract number W15P7T-10-C-F600

XCCDF
security
benchmark
automation

Thank You!

Supported by NSA contract number W15P7T-10-C-F600