XCCDF Developer Workshop

Winter 2010 Security Automation Developer Days

Feb. 23, 2010

Charles Schmidt – The MITRE Corp.

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

Objectives

- **There are currently 31 open issues tracked for XCCDF**
  - Range from complex topics to simple fixes
- **Try to resolve as many issues as possible today**
- **Following today's discussion**
  - Minutes of discussions
  - Detailed proposals for all topics that reached consensus
  - Going forward, a complete XCCDF schema/spec that covers all agreed-upon changes

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

Issue Categories

- **Discussion topics (18)**
  - Some will require significant discussion, but many are expected to be relatively simple issues
- **Fix Proposals (10)**
  - Straightforward – no discussion expected
  - Included to keep the community informed

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

XCCDF security benchmark automation

Agenda

- Using CVSS/CCSS in scoring
- Updating use of CVSS/CCSS in the impact-metric
- Updating the use of CPE
- Explicit mapping of check results to XCCDF results
- Segregated or mixed extensions to Value
- Content categorization
- check-import
- Opening the metadata field
- Using Dublin Core in the status field
- The "role" field
- Clarifying requires/conflicts processing
- check-content-refs without names and the "multiple" property
- check-content-refs to XCCDF documents
- Profile selector order-of-operation
- "Default" values in Values
- Local vs. Remote schema imports
- Enumerated notice types
- Stand-alone TestResults
- Review of simple fixes

There will be a 1-hour break for lunch at 12:30

MITRE

Using CVSS/CCSS in Scoring Discussion Topic

- **New scoring model that uses CVSS/CCSS scores**
  - Will such a scoring model be useful?
  - Should temporal/environmental scores factor in? If so, how would they be included?
    - Part of tailoring?
    - Included in profile?
    - Allow to be implementation-specific?
  - How would the CVSS/CCSS scores be used in an algorithm?

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

Using CVSS/CCSS in Scoring Sample Proposal

= Use impact-metric field (no new field needed)

Δ "Flat metric" – sum of all CVSS/CCSS scores associated with scored Rules that do not pass

Δ "Percentage metric" – percent of total possible CVSS/CCSS score (sum of all scored Rules) that passed

Δ For scoring only, use a default score of 6.0 if no impact-metric field (i.e. an average-impact, remotely-exploitable issue)

= Impact-metric is base score only - tools may create proprietary means for adding temporal/environmental

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

Updating impact-metric Discussion Topic

- **Currently only CVSS base vectors allowed - Add CCSS? Add temporal/environmental?**
  - Adding temporal/environmental reduces generality and increases computational complexity
  - How do we handle versioning of CVSS/CCSS?
  - Do we want the schema to enforce formatting?

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

Updating impact-metric Sample Proposal

- Δ Allow CCSS vectors
- = Restrict Benchmarks to base vectors – tools may develop proprietary ways to tailor in other vectors
- = No version info in schema - specification requires CVSS 2 or CCSS 1
- Δ Use restriction to force impact-metric to follow CVSS/CCSS
  - Δ <xsd:pattern value="AV:[LAN]/AC:[HML]/Au:[MSN]/C:[NPC]/I:[NPC]/A:[NPC](/PL:[RUA]|(ND)/EM:[AP])?"/>

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

Updating the use of CPE Discussion Topic

- **XCCDF requirement to use CPE 2.0 is out of date**
  - How flexible do we want the specification to be?
    - Require CPE 2.2 (with support for a few deprecated formats)?
    - Permit a specific range of versions but still focus on one format (i.e. CPE 2.x)?
    - More flexible platform specification?

Updating the use of CPE Sample Proposal #1

Focus on CPE 2.x

Δ The specification will be updated to require use of CPE version 2.x

= Other deprecated formats will remain available

– Challenge: Lack of forward compatibility where a tool is able to understand CPE 2.2 but becomes confused by later XCCDF documents written using CPE 2.3, or later

- Tool authors must keep their XCCDF tools up to date with CPE to remain current

Updating the use of CPE Sample Proposal #2

Support Named Platform Identifiers: Allow benchmark authors to identify platform identifier type/version

- New platform element that could hold arbitrary XML (its body) or a string (in an attribute)
  - Allows any format of platform identifier
- Explicitly name the platform ID language using a new @system attribute

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

Map Check Results to XCCDF Discussion Topic

- **Mapping check results to the different XCCDF results**
  - Do we need to explicitly map results to each and any result types, or just to pass or fail?
  - Can we assume there is always a “pass” and “fail” in the checking language?
    - If so, is it sufficient to allow negating the default mapping?
  - Checking languages may have many result types
    - Want shorthand methods to map many checking language results to one XCCDF result?

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

Map Check Results to XCCDF Sample Proposal

- A new optional element will be added to the checkType, called ‘check-result-map’
- Check-result-map will have a required attribute called "result" that must contain an XCCDF result
- The body of this element is a string and would correspond to a return result from the checking system
- Any number of check-result-map elements may appear but no two elements may have the same body value
- Lack of explicit mapping defaults to standard mappings (800-126 or from checking language) or Unknown

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

Segregated or Mixed Extensions Discussion Topic

- **Allow lists/external types in XCCDF Values**
  - Prior proposal adds lists and external types to Value types
  - Should a single Value only have one kind of type?
    - Only singletons (current) or only lists/external (new)
  - Is it better to allow Value to be tailored to either kind of type?

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

Content Categorization Discussion Topic

- **Rules/Groups categorized by two one-to-many relations: Group position or cluster-id**
  - Request for ways to express arbitrary many-to-many relationships
  - Is this functionality useful?
  - Create new structures or revise cluster-id to support many-to-many relations?

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

Content Categorization Sample Proposals

- Δ 1: Add new “category” element to Items
  - Δ Any number of category elements, each a keyword/categorization
  - Δ Category names could be any string, including multiple-word phrases
  - Δ Inherited under the "append" processing model
  - = Plays no role in tailoring or assessment
- Δ 2: Expand the use of the cluster-id attribute to hold a list
  - = Categories must be NCNames (1 word)
  - = Not inherited
  - = Allows tailoring by any keyword/categorization
    - Δ Improves likelihood of one Item getting tailored multiple times in a Profile

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

XCCDF security benchmark automation Check-import Discussion Topic

- **Check-import element is under-defined**
  - What should be the purpose of check-import?
    - Archiving discovered info
    - Populating Values for later export
  - If importing data for subsequent export how would we get around issues of Value dependency?
    - Small scope
    - Trace and follow dependencies

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

Check-import Sample Proposals

- = 1. Check-import as an archiving tool
  - = Check-import identifies check structure to be recorded in test-result

- Δ 2. Check-import for Value population
  - Δ Add field to identify a Value
  - Δ Imports only in scope within a Rule

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

Opening the Metadata Field Discussion Topic/Proposal

- **XCCDF schema limits metadata field to Dublin Core and NIST Checklist (SCCF) formats**
  - Allow to use additional metadata information?
  - Should strict processing still be required?
- **Sample Proposal**
  - Δ Remove references to specific schemas
  - Δ Allow lax processing to support ad-hoc metadata

Dublin Core in the Status Field Discussion Topic/Proposal

- **Request to include Dublin Core info in status**
  - Just Dublin Core or other metadata formats too?
  - Is the status element the correct place for this?
    - Status field is a simpleType so using status field requires loss of existing text restrictions

- **Sample proposal**
  - Δ Add a metadata field with the metadataType type to Items

The “role” Field Discussion Topic/Proposal

- **Clarify use of selected vs. role="unchecked" vs. UNCHECKED rule result**
  - How do we handle multiple sources of “unchecked” result?
  - How does role fit in the Item processing model
- **Sample proposal**
  - Δ Deprecate the role property
    - = Role would not be removed until the next major release of XCCDF, but its use would be discouraged
  - = Current role functions can be done with other methods

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

XCCDF security benchmark automation — Requires/conflicts Processing Discussion Topic/Proposal

- **There are unintuitive results in current requires/conflicts resolution**
  - What is the purpose of the requires/conflicts statements? Follow explicit or implicit selection?
  - Is the simplicity of the current model worth having somewhat counter-intuitive behaviors?
- **Sample Proposal**
  - Δ Change the instructions for Item.Process to also check for containing Group selection
  - = Don't follow transitive dependencies
    - = We still get some unintuitive results, but full fix is costly

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

Check-content-refs Names Discussion Topic

- **What do we do with a missing name in check-content-ref?**
  - There is existing content that does this – don't deprecate
- **Clarify the multiple property of XCCDF rules**
  - Does this refer to references to multiple checks?
  - Does this refer to references to a single check with multiple targets?
  - How should component checks be combined if the multiple property is false?

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

Check-content-refs Names Sample Proposal

- Multiple deals with references to multiple checks (refs without names)
  - If multiple is true each component check creates an “implicit Rule”
  - Each implicit Rule would appear in their own rule-results entry in the TestResults
    - Same ID; other fields would distinguish
- If the "multiple" property is false, all component checks are ANDed together

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

Check-content-refs to XCCDF Discussion Topic/Proposal

- **XCCDF check-content-ref statements referring to other XCCDF documents**
  - How do we handle XCCDF tailoring?
  - XCCDF-check relationship now not strictly hierarchical
- **Sample proposal**
  - Δ Add new optional element called "check-control"
    - Δ Holds info in XML structure passed on to interpreter
  - Δ Checking languages define their own control schemas
  - Δ XCCDF would define a control schema to allow tailoring

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

Profile Selector Order Discussion Topic

- **Issues discovered with recent selector proposal**
  - Intent was to allow extension to override behavior, but the order of application complicates this
  - Do we wish extension to allow Profile overrides?
  - Is the prohibition against duplicate selectors (same selector with same ID) necessary?
  - Should extension of Profiles be allowed to control location of extending selectors?

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

Profile Selector Order Sample Proposals

- Three options
  - = 1. Selectors are appended during extension but no overlapping selector-idref pairs are permitted
    - = No overriding
  - Δ 2. Selectors replace in the case of overlapping selector-idref pairs and append otherwise
    - Δ Overriding but with some complexities
  - Δ 3. Append but allow duplicates
    - Δ Overriding but possible repeated tailoring of an Item

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

XCCDF "Default" values in Values Discussion Topic/Proposal

- **Unclear how to treat Value fields without prior tailoring**
  - Mark default with a selector or should we create a separate attribute that denotes a default?
    - Rules make empty/absent selector property the default
  - What if no default "value" since a value is required?
- **Sample Proposal**
  - Δ Pre-tailoring, fields with non-empty selectors will be ignored
    - Δ The exception is the value element – if no default, use the first value that appears in the XML
  - Δ Add uniqueness constraints for all tailorable Value fields

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

Local v Remote Schema Imports Discussion Topic/Proposal

- **Import from local files or canonical remote locations?**
  - Local files require bundles but avoid network requirements
  - Remote files ensure canonical source
  - How do we handle versioning of referenced schemas?
  - Do we need just one answer? Can we pick & choose?
- **Sample proposal**
  - Self explanatory

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

Enumerated Notice Types Discussion Topic/Proposal

- **Multiple uses of the notice field**
  - Request to annotate notices to allow for different presentation styles
  - Given that presentation will be implementation dependent, is this worthwhile?
- **Sample Proposal**
  - Δ Add “type” attribute to notice type
  - Δ Possible values: copyright, warning, license, general
  - Δ Default is “general”

Stand-alone TestResults Discussion Topic/Proposal

- **How should we handle sets of TestResults**
  - Currently one per file or include referenced Rules
  - Do we want to be able to hold many TestResults without requiring their referenced Rules?
  - If TestResults will live alone, what other information must they contain? (E.g. Metadata?)
- **Sample Proposal**
  - Δ Create a new root element called BenchmarkResults
    - Δ Can hold results from different assessments and/or different Benchmarks
  - Δ Add an optional metadata element to testResultType

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

Fix Proposals

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

Update Truth Tables

AND	**P**	**F**	**U**	**E**	**N**	**K**	**S**	**I**
P	P	F	U	E	P	P	P	P
F	F	F	F	F	F	F	F	F
U	U	F	U	U	U	U	U	U
E	E	F	U	E	E	E	E	E
N	P	F	U	E	N	N	N	N
K	P	F	U	E	N	K	K	K
S	P	F	U	E	N	K	S	S
I	P	F	U	E	N	K	S	I

OR	**P**	**F**	**U**	**E**	**N**	**K**	**S**	**I**
P	P	P	P	P	P	P	P	P
F	P	F	U	E	F	F	F	F
U	P	U	U	U	U	U	U	U
E	P	E	U	E	E	E	E	E
N	P	F	U	E	N	N	N	N
K	P	F	U	E	N	K	K	K
S	P	F	U	E	N	K	S	S
I	P	F	U	E	N	K	S	I

	P	**F**	**U**	**E**	**N**	**K**	**S**	**I**
not	F	P	U	E	N	K	S	I

P = Pass
F = Fail
U = Unknown

E = Error
N = NotApplicable
K = NotChecked

S = NotSelected
I = Informational
X = Fixed (treat as P)

Remove reference to check-export

DOCUMENTATION: Page 51

When a check element is a child of a Rule object, check-import and check-export elements must be empty.

Changes to:

When a check element is a child of a Rule object, the check-import element must be empty.

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

Fix <references> description

DOCUMENTATION Page 68:

<reference>

...

Content:	string or elements
Cardinality:	0-n
Parent Elements:	Benchmark, Group, Rule, Value, Profile
Attributes:	~~**xml:lang,**~~ href
Child Elements:	*none or Dublin Core Elements*

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

Fix <description> description

DOCUMENTATION: Page 55

<description>

This element provides the descriptive text for a Benchmark, Rule, Group, or Value. It has ~~no~~ **two** attributes: **xml:lang and override**. Multiple description elements may appear with different values for their xml:lang attribute (see also next section).

Remove non-existent field

DOCUMENTATION: Page 36 –

Sub-Step	Description
Item.Select	If any of the following conditions holds, cease processing of this Item. 1. The processing type is Tailoring, and the ~~**optional property and**~~ selected property ~~**are both**~~ **is** false. 2. The processing type is Document Generation, and the hidden property is true. 3. The processing type is Compliance Checking, and the selected property is false. 4. The processing type is Compliance Checking, and the current platform (if known by the tool) is not a member of the set of platforms for this Item.

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

Redundant cluster-id def

DOCUMENTATION: Page 18 – Removing cluster-id from description of Group

Group :: Item

Property	Type	Count	Description
requires	identifier	0-n	The id of another Group or Rule in the Benchmark that must be selected for this Group to be applied and scored properly
...	...	...	...
platform	URI	0-n	Platforms to which this Group applies, CPE Names or CPE platform specification identifiers
~~**cluster-id**~~	~~**identifier**~~	~~**0-1**~~	~~**An identifier to be used from Benchmark profiles to refer to multiple Groups and Rules, optional**~~
extends	identifier	0-1	An id of a Group on which to base this Group

DOCUMENTATION: Page 45 – Removing cluster-id from Group dictionary entry

A Group element contains descriptive information about a portion of a Benchmark, as well as Rules, Values, and other Groups. A Group must have a unique id attribute to be referenced from other XCCDF documents or extended by other Groups. The id attribute must be a unique identifier. The 'extends' attribute, if present, must have a value equal to the id attribute of another Group. ~~**The 'cluster-id' attribute is an id; it designates membership in a cluster of Items, which are used for controlling Items via Profiles.**~~ The 'hidden' and 'allowChanges' attributes are of boolean type and default to false. The weight attribute is a positive real number.

Loading.Resolve for Items and Profiles

DOCUMENTATION: Page 34

Sub-Step	Description
Loading. Noticing	For each notice property of the Benchmark object, add the notice to the tool's set of legal notices. If a notice with an identical id value is already a member of the set, then replace it. If the Benchmark's resolved property is set, then Loading succeeds, otherwise go to the next step: Loading.Resolve.Items.
Loading.Resolve. Items	For each Item in the Benchmark that has an extends property, resolve it by using the following steps: (1) if the Item is Group, resolve all the enclosed Items, (2) resolve the extended Item, (3) ~~**prepend the property sequence from the extended Item to the extending Item**~~ **insert the necessary property sequences from the extended Item into the appropriate locations in the extending Item** (4) if the Item is a Group, assign values for the id properties of Items copied from the extended Group, (5) remove **all but the last instance of** duplicate properties and apply property overrides, and (6) remove the extends property. If any Item's extends property identifier does not match the identifier of a visible Item of the same type, then Loading fails. If the directed graph formed by the extends properties includes a loop, then Loading fails. Otherwise, go to the next step: Loading.Resolve.Profiles.
Loading.Resolve. Profiles	For each Profile in the Benchmark that has an extends property, resolve the set of properties in the extending Profile by applying the following steps: (1) resolve the extended Profile, (2) ~~**prepend the property sequence from the extended Profile to that of the extending Profile**~~ **insert the necessary property sequences from the extended Profile into the appropriate locations in the extending Profile,** (3) remove all but the last instance of duplicate properties. If any Profile's extends property identifier does not match the identifier of another Profile in the Benchmark, then Loading fails. If the directed graph formed by the extends properties of Profiles includes a loop, then Loading fails. Otherwise, go to Loading.Resolve.Abstract.

Ordering of Benchmark contents

DOCUMENTATION: Page 16

Conceptually, a Benchmark contains Group, Rule, and Value objects, and it may also contain Profile and TestResult objects. For ease of reading and simplicity of scoping, all Value objects must precede all Groups and Rules, which must precede all Profiles, which must precede all TestResults. These objects may be directly embedded in the Benchmark, or incorporated via W3C standard XML Inclusion [10].

Changes to:

Conceptually, a Benchmark contains Group, Rule, and Value objects, and it may also contain Profile and TestResult objects. For ease of reading and simplicity of scoping, all Profiles must precede all Groups, Rules, and Values. Groups can contain Values, Rules, and other Groups. Within any level of the Group hierarchy (including at the top level, within the Benchmark itself), Values must precede sibling Groups and Rules. All Values, Groups, and Rules must precede all TestResults. These objects may be directly embedded in the Benchmark, or incorporated via W3C standard XML Inclusion [10].

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

Document selector attribute in refine-rule

DOCUMENTATION: Page 28

refine-rule – a Rule/Group selector. This selector allows the Profile author to **select check statements,** override the scoring weight, severity, and role of a Rule, Group, or cluster of Rules and Groups. Despite the name, this selector does apply for Groups, but only to their weight property.

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

Typo in Profile description

DOCUMENTATION: Page 48 – <Profile> Updating Profile dictionary to reflect four selectors

A Profile element encapsulates a tailoring of the Benchmark. It consists of an id, descriptive text properties, and zero or more selectors that refer to Group, Rule, and Value objects in the Benchmark. There are ~~**three**~~ **four** selector elements: select, set-value, **refine-rule,** and refine-value.