OVAL Developer Days

July 18-19, 2005

The MITRE Corporation
Bedford, MA

Agenda (v1.0)

Monday July 18th 2005

10:00 - 10:15 **welcome**

- *Introductions*
- *Goals for the next two days*
- *Outline current issues with Version 4 of the OVAL Schema*

10:15 - 12:00 **v5 working session**

- *Proprietary definitions*

  While MITRE is currently the sole source of OVAL Definitions, we understand that there could soon be a number of organizations generating their own content, which will cause problems with the current definition and test ID format. The OVAL identification scheme should be structured, such that they can be associated with a specific organization via a standardized format.

  - Topics:
    - new OVAL ID format to distinguish between organizations
    - xml signatures to sign each definition
    - support the building block approach of modifying existing definitions

- *Combining definitions and tests*

  The criteria section of a definition performs a similar function to a compound test. If we were to convert the criteria section into a compound test, this would allow us to treat definitions like tests, and embed them directly in other definitions.

  - Topics:
    - remove the criteria and just reference a compound test
    - value of software and configuration sections
    - the purpose of definitions and tests and what each is trying to accomplish

12:00 - 1:00 **lunch MITRE café**

1:00 - 2:45 **v5 working session**

- *TRACK 1 - Breaking out the objects*

  How can OVAL be used to test a complex set of objects? Under the current design, there are problems trying to specify conditions like all the users of a certain group, or all directories that contain a certain file. By pulling the object declaration out of a test, can we develop a structure that allows for this complexity to be handled?

  - Topics:
    - separate the object section from the test
    - allow multiple tests to reuse same object
    - ability to create complex object descriptions
    - addition of behavioral identifiers to guide the collection

- *TRACK 2 - Discuss requirements for OVAL Compatibility*

  Currently, the OVAL Compatibility program is loosely defined. With a number of companies making their compatibility intentions known, it is time to formalize this process. What is realistic within the community and how will companies achieve the compatibility goal?

  - Topics:
    - relation to the Definition, System Characteristic, and Results Schemas
    - meaning of compatibility to producers and consumers
    - verification options to test compatibility

3:00 - 3:30 **discussion**

A round-table discussion about the different experiences within the community of working with the OVAL Schema, both good and bad. What roadblocks were encountered during tool development and how were the issues resolved?

3:45 - 5:00 **v5 working session**

- *Patching definitions*

  While much of the information contained within a patch definition is similar to that within a vulnerability definition, the structure and meaning of this information is quite different. OVAL first needs to get a handle on the unique problems that will be encountered within this class of definitions, and determine how the language can be adapted to solve them.

  - Topics:
    - the type of information included in a patch definition
    - superseding patches
    - work through an example

5:00 - 5:30 **wrap-up**

- *Summary of day's accomplishments*

6:30 - 8:00 **dinner at Naked Fish**

Tuesday July 19th 2005

8:00 - 9:30 **v5 working session**

- *Results Schema*

  One of the biggest areas of interest in OVAL thus far, has been the Results Schema. This interest has raised a number of questions about the future direction of this schema. It is time to take a step back and revisit the Results Schema and examine its goals, purpose, and use. Given a clean slate, what requirements would define the structure of this schema? How can we modify the existing format to meet some of these requirements?

  - Topics:
    - how is the results file being used?
    - is the current format too verbose?
    - aggregated results flag
    - supporting multi-host output

- *Pass/fail logic for tests*

  There seems to be a growing need for expanding the set of operators available to definition producers – the current set consists of AND, OR, and XOR. For example, configuration specific OVAL definitions often require testing that a software component exists prior to testing if the configuration of that software is in compliance.

  - Topics:
    - addition of ONPASS and ONFAIL operators
    - relation to existing software and configuration sections
    - improving the results by reporting "NOT TESTED" instead of "FAILED"
    - introduction of new operators (e.g. COUNT, IN, RANGE)

9:45 - 10:15 **discussion**

A round-table discussion about the OVAL development process. How is the current scheduling of schema releases working for everyone? What changes could be made to streamline the entire process?

10:30 - 12:00 **v5 working session**

- *TRACK 1 - OVAL variables*

  The recent compliance definition work by The Center for Internet Security (CIS) has made heavy use of OVAL Variables. As a result of this work, shortcomings in the current implementation have been identified, and improvements have been suggested. We would like to discuss these suggestions, as well as other potential enhancements to this function.

  - Topics:
    - replace existing component type
    - allow the output of one test to be used by another
    - interaction with other languages

- *TRACK 2 - Expanding the Adoption of OVAL*

Increasing the community adoption of OVAL is a difficult and never-ending task. Now that OVAL has started to gain acceptance in the security community, how do we keep up the momentum? Also, are there areas of the industry in which OVAL would be applicable, which have yet to be explored?

- Topics:
  - promoting within the industry
  - identify and integrate with other standards efforts

12:00 - 1:00 **lunch MITRE café**

1:00 - 2:45 **v5 working session**

- *Lightweight definition writer*

  Would it be beneficial to develop a tool to assist content creators? The goal of such a tool would be, to speed up the creation of new content and to facilitate sharing and reuse of existing tests.

  - Topics:
    - web-based vs. stand-alone
    - features that would be needed

- *Web services*

  In an effort to assist OVAL tools with performing many common tasks related to OVAL, MITRE would like to provide a set of web services. Would this be useful for the community and what services would be desired?

  - Topics:
    - content distribution
    - OVAL analysis
    - automated content submission

- *Break the OVAL Definition Interpreter into smaller 'engines'*

  While we see the Interpreter as beneficial to providing an example of OVAL in use, would it be beneficial to develop a more modular design to allow easier reuse of specific components by other tools? Is there a set of components currently not contained within the Interpreter that would be useful? The goal would be to help organizations integrate OVAL into their tools..

  - Topics:
    - to be used as plug-ins
    - easy development of OVAL-compatible systems

- *Namespace and version info*

  Part of facilitating the development of OVAL tools is enabling applications to handle new versions of the schema. How should namespaces and version info be used to help?

  - Topics:
    - should we have version info in namespace?

3:00 - 3:30 **wrap-up**

- *Summary of day's accomplishments*