HS SEDI
Homeland Security Systems Engineering and Development Institute

Open Vulnerability and Assessment Language

OVAL®

Status Update

Jon Baker
September 28, 2010

Homeland Security

OVAL Overview

An international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services.

- **Open Vulnerability and Assessment Language**
  - A community-developed open standard
  - Began in December 2002
- **OVAL Language**
  - XML-based framework for making logical assertions about a system
    - Vulnerable, Compliant, Installed application, Patched
  - OVAL Interpreter
    - An open source reference implementation
- **OVAL Repository**
  - collection of community contributed OVAL Definitions
- **OVAL Adoption**
  - both educate vendors and receive constructive technical feedback

MITRE's Role in OVAL

- **MITRE is a not-for-profit corporation, chartered to work solely in the public interest.**
  - MITRE operates Federally Funded Research and Development Centers (FFRDCs).
  - Non-compete charter fosters "trusted moderator" status.
  - Work in the public interest.
  - Government sponsored.

- **OVAL Moderator**
  - Help drive consensus between government customers and greater community with technical solutions and changes.
  - Promote the **growth and adoption** of OVAL.
  - **Listen** to the community and guide the development of OVAL.
  - **Facilitate** the OVAL Board.
  - **Moderate** the OVAL Repository.
  - **Balance different perspectives** to arrive at the consensus solution that is best for OVAL and the public interest.

OVAL Releases

- Minor releases add tests, minor capabilities, and critical fixes.
- Releases occur as needed by the community (2-3 per year).
- All releases are approved by the OVAL Board.

- **Version 5.0**
  - Release Date: June 16, 2006
- **Version 5.1**
  - Release Date: November 6, 2006
- **Version 5.2**
  - Release Date: January 31, 2007

SCAP 1.0

- **Version 5.3**
  - Release Date: June 27, 2007
- **Version 5.4**
  - Release Date: April 10, 2008

- **Version 5.5**
  - Release Date: October 1, 2008
- **Version 5.6**
  - Release Date: September 11, 2009
- **Version 5.7**
  - Release Date: May 12, 2010
- **Version 5.8**
  - Release Date: September 15, 2010
- **Version 5.9**
  - Planning Started: September 15, 2010
- **Version 6.0**
  - Planning: TBD

SCAP's Use of OVAL

- **OVAL provides the low level system assessment capability.**
  - SCAP Validated products use OVAL Definitions as the basis for system assessments (patched, vulnerable, compliant, compromised, application installed).

- **OVAL's Use Cases**
  1. **Security Advisory Distribution -** Defining the conditions under which the issue exists.
  2. **Vulnerability Assessment -** Detecting the presence of the issue.
  3. **Patch Management -** Determining if the patch can be installed.
  4. **Configuration Management -** Defining the desired configuration and monitoring systems.
  5. **Auditing and Centralized Audit Validation -** Representing detail system assessment results over time.
  6. **Security Information Management Systems (SIMS) -** Standardized assessment result format for consumption and fusion with other sensor inputs.
  7. **System Inventory -** Describing how to detect an installed application.
  8. **Malware and Threat Indicator Sharing -** Describing the possible locations of malware or threat artifacts and indicators.

What’s new for OVAL 5.5?

- **Corrected documentation and Schematron errors.**
  - Search scope limited to SACL/DACL when checking permissions in Windows.
  - Data types are based on XML Schema data types.
  - Clarified 'version' datatype format.
  - Require @var_check when a @var_ref is used.
- **Added several new functions.**
  - arithmetic, regex_capture, time_difference
- **Added Cisco PIX OS component schema.**
- **Added and corrected several tests.**
  - win-def:wuaupdatesearcher_test
  - win-def: user_sid55_test
  - ios-def:version55_test
  - catos-def:version55_test
  - catos-def:line_test

What's new for OVAL 5.6?

- Allow pattern matches on elements that are restricted to an enumeration.
- Allow a test to reference multiple states for more sophisticated state comparisons.
- Introduced a choice structure inside of objects to allow files to be defined by either a path and filename or simply a complete file path.
- Changed the required regular expression syntax to Perl 5's regular expression specification.
- Deprecated the resolve_group behavior on all tests in the Windows component schema except for the sid_sid_test and the sid_test.
  - helps to avoid overly resource-intensive searches for Windows trustees.
- New Tests and Component Schemas Added in Version 5.6
  - Added the win-def:serviceeffectiverights_test to support checking the rights of services on Windows.
  - Added the ind-def:ldap_test to support checking settings via LDAP queries to a directory server.
  - Added the aix-def:interim_fix_test to support checking interim or emergency fixes on IBM AIX.
  - Added the SharePoint component schema.
  - Added a new patch test to the VMware ESX component schema.

Tests Reference Multiple States

- **A single item can be tested against multiple states.**
  - Allows for the expression of ranges of acceptable values.
  - Specify multiple acceptable values.
  - Simplifies content authoring.

- **What Changed?**
  - Introduced a new @state_operation on the oval-def:TestType.
  - Changed the multiplicity of states in the oval-def:TestType.

- **Example: Minimum password length is between 8 and 16**
  - Items must satisfy state 1:

```
<min_passwd_len datatype="int" operation="greater than or equal">8</min_passwd_len>
```

  - AND state 2:

```
<min_passwd_len datatype="int" operation=“less than or equal">16</min_passwd_len>
```

What's new for OVAL 5.7?

- **Added support for n-tuples.**
- **Numerous Schematron rule refinements and performance focused improvements.**
  - Introduced Schematron phases.
- **Significant documentation improvements were made throughout the OVAL Language.**
- **Removed deprecated items.**
  - ind-def:filemd5_test and apache-def:version_test
- **Added new tests.**
  - Added the win-def:dnscache_test and unix-def:dnscache_test
  - Added new tests in order to leverage n-tuple support.

N-Tuples

- **A record comprised of any number of related fields can be represented and tested in OVAL.**
  - Example Pair: {Name, ScreenSaverTimeOut}
  - Improves support for WMI, XML, SQL, and other complex data stores.

- **What Changed?**
  - Introduced a new structure to represent a record.
  - Updated WMI, SQL, XML, Active Directory related tests to leverage the new record structure.

- **Example:**

WQL - SELECT Name, ScreenSaverTimeOut FROM Win32_Desktop;

```
<wmi_state id="oval:sample:ste:2" operator="AND" version="1" xmlns=“…“>
   <result datatype="record" operation="equals" >
      <field name= "Name" datatype="string" operation="equals">user2</field>
      <field name= "ScreenSaverTimeOut" datatype="int" operation="less than">600</field>
   </result>
</wmi_state>
```

What’s new for OVAL 5.8?

- Refactored datatype constraints on all entities.
- Added support for unbounded filter elements in objects.
- Added an explicit mapping of tests, objects, states, and items.
- Added an OVAL Directives schema.
- Enhanced OVAL Results directives.
- Added many new tests and entities to the Windows, UNIX, Linux, Solaris, and Mac OS component schemas.
- Corrected inconsistencies across item, object, and state entity names, types, and multiplicity.

Refactored Datatype Constraints

- **Datatype restrictions are now primarily enforced with XML Schema.**
  - Removed thousands of Schematron rules.
  - Simplified document validation.
  - Improved schema readability and maintenance.
  - Leading to higher quality OVAL Content.

- **What changed?**
  - Added a xsd:fixed attribute to most entity declarations

```
<xsd:attribute name="datatype" type="oval:SimpleDatatypeEnumeration" use="required" fixed="binary"/>
```

Filters on Objects

- **The set of OVAL Items that match an OVAL Object can be filtered by any relevant property of the OVAL Item.**
  - Huge savings of processing time and memory usage.
  - Greatly reduces the size of an OVAL Results document and helps to limit the results to only the important information.

- **What Changed?**
  - Added an optional filter element to all OVAL Objects.

    ```
    <xsd:element ref="oval-def:filter" minOccurs="0" maxOccurs="unbounded"/>
    ```

    - Leverages the existing filter concept.
    - Data collectors need to apply each filter to determine if an Item matches.

- **Example: World writable files are not permitted**
  - Before filters on Objects – Data collection on a test system resulted in OVAL Items for 148745 files.
  - With filters on Objects – Data collection on a test system resulted in OVAL Items for 1254 files.

OVAL Results Directives

- **Allows for tailoring of OVAL Results to include only the relevant information.**
  - No need to include source OVAL Definitions.
  - Control OVAL Results by type of OVAL Definition and result value.
  - Defined format for specifying the directives to be used during evaluation

- **What Changed?**
  - Added an attribute to explicitly indicate whether the source OVAL Definitions document should be included in the OVAL Results or not.
  - Added optional directives by definition class.
  - Added a new standalone directives document.

- **Example:**
  - 2,293KB – Full OVAL Results for FDCC on Windows XP
  - 1,110KB – Tailored OVAL Results for FDCC on Windows XP
    - Excludes source OVAL Definitions
    - Minimal details for true compliance results and inventory results
    - Full details for compliance failures

OVAL Repository

The central meeting place for the community to discuss, analyze, store, and disseminate OVAL Definitions.

- **Active community contributing OVAL Definitions for the latest vulnerabilities.**
- **Coverage for a diverse set of applications and operating systems**
  - Microsoft, Debian, Mozilla, Solaris, Adobe, Apple, and more...
- **10,000 Definition Milestone – September 16, 2010**

Other Public Repositories of OVAL content

debian NIST Novell. redhat

OVAL Adoption

Total Participants:
Organizations: 17
Products & Services: 25

- **Provides a channel to both educate organizations about OVAL and receive constructive technical feedback to evolve the standard.**
  - Best practice usage guidance
  - Vendor formal self-assertions
  - Provides MITRE deeper insights into how OVAL is or could be utilized

- **Defines requirements for how to use OVAL.**
  - Authoring Tool
  - Definition Evaluator
  - Definition Repository
  - Result Consumer
  - System Characteristics Producer

Get Involved!

- **Come to the OVAL Workshop**
  - Explore the need for a major revision and other future considerations for the OVAL Language.
  - Wednesday from 2:15pm – 3:00pm

- **Join the OVAL mailing lists**
  - **OVAL-Announce** – General news and announcements about OVAL
  - **OVAL Developer's Forum** – Public forum for discussing the OVAL Language, addressing OVAL implementation issues, and for assisting other developers with OVAL.
  - **OVAL Repository Forum** – Public forum for discussing OVAL Repository content.

    https://oval.mitre.org/community/registration.html

- **Participate in the OVAL Adoption Program**
  - Help shape the effort

    https://oval.mitre.org/adoption/