OVAL Board Meeting (7/13/2009)

Attendees

Jonathan Baker – MITRE
Andrew Buttner – MITRE
Danny Haynes – MITRE
Mike Lah – MITRE

Melissa Albanese – DoD
James Hansen – BigFix, Inc.
Kent Landfield – McAfee
Anton Chuvakin – Qualys, Inc.
Nick Connor – Assuria Limited
Chris Wood – Assuria Limited
Jay Graver – nCircle Network Security, Inc.
Rob Hollis – ThreatGuard, Inc.
Dennis Moreau –EMC
Blake Frantz – CIS
Mark Cox – Red Hat
Pai Peng – Hewlett Packard

Meeting Summary

Welcome

The group was welcomed and thanked for attending the 2009 3rd quarter OVAL Board Meeting. One new board member was introduced to the group:

- James Hansen – BigFix, Inc.

Status Update

A status update of the OVAL project as a whole was delivered. The following items were covered:

- OVAL Language
  - We have been busy working on Version 5.6 Draft 2 of the OVAL Language which was released on July 2, 2009.
  - On July 17, 2009, we will post the Version 5.6 Release Candidate unless the release date is pushed back due to the decision to add n-tuples into Version 5.6 of the OVAL Language.
  - We would like to discuss these changes and obtain feedback from the OVAL Board.
- OVAL Interpreter
  - The majority of the work performed on the OVAL Interpreter was to improve support for the Windows and UNIX tests.
  - The next build of the OVAL Interpreter is planned for release on July 26, 2009.

    - We would appreciate any testing of the OVAL Interpreter prior to the release of the build and would be willing to provide anyone interested with a pre-release build.
    - We continue to be focused on developing a single-host reference implementation OVAL Interpreter in order to provide a complete reference that demonstrates the OVAL Language.
    - The new build will feature many new tests including the win-def:activedirectory_test, win-def:interface_test, and the win-def:sharedresource_test.
- OVAL Repository
    - The top contributor this quarter was SecPod Technologies.
    - We did a large scrub of the OVAL Repository metadata.
    - We have a new team member, Mike Lah, who will be taking over maintaining the OVAL Repository infrastructure.

OVAL Developer Days Recap

The OVAL Developer Days Conference, as well as the Security Automation Conference, was a great success. On average, there were 60 to 70 attendees present on each day of the conference. As a result of the discussions at the OVAL Developer Days Conference, the following action items emerged.

Deprecation Policy Clarification

There is a need to clarify the deprecation policy and to state that Schematron rules do not fall under the deprecation policy.

Supporting Multiple Versions in Parallel

There is a strong desire to support the development of multiple version of the OVAL Language in parallel. This will require further discussion with the sponsor-base in order to help support the needs of the OVAL Community. We encourage members of the OVAL Community to post proposals for this topic on the oval-developer-list.

Defining a Major and Minor Version

There is a need to clarify the difference between major and minor releases of the OVAL Language as well as define how much can we add to an OVAL release before it becomes a major change.

OVAL Specification

There are requests for an OVAL Language specification. Currently, we rely on the OVAL schemas and documents that contain high-level overviews, but, we have never had a formal specification. There have been requests for more formal and refined documentation which is indicative of the success of the OVAL Language.

OVAL Language Versioning Process and Implementation Review

There is a request to encode both the major and minor release versions within the XML namespaces that allows for the differentiation of tests across versions. The current versioning methodology can be found at http://oval.mitre.org/language/about/versioning.html. There is a need to expand the "Differentiating Language Versions" section such that it is clarified. Originally, it was intended that the convention used in the namespaces followed XML best practices. However, it is possible that the best

practices have changed. Therefore, we will look into this issue and post our findings to the oval-developer-list. A conference call can be scheduled, if necessary, to discuss any potential changes to the versioning implementation of the OVAL Language.

Security Automation Conference Minutes

The minutes for the 2009 Security Automation Conference, including OVAL, are posted on the Making Security Measurable website. In general, the minutes have been lengthy and in-depth. Many OVAL Board members found the minutes very useful. The minutes will also be distributed to the oval-board-list.

OVAL Version 5.6 Review Process

Draft two of Version 5.6 of the OVAL Language is now available on the OVAL website. On July 17, 2009, the release candidate for Version 5.6 of the OVAL Language will be made available and posted on the OVAL website. The Version 5.6 release of the OVAL Language will contain many changes. Therefore, a board review, and subsequent approval, of the release candidate will be critical for a solid release of the OVAL Language.

OVAL Version 5.6 Highlights

Choice Structure on Objects

As a result of the Security Automation Conference, a consensus was reached indicating that the introduction of the choice structure on objects will be beneficial to the OVAL Language. The choice structure was first introduced in Draft 2 of the OVAL Language. Currently, the choice structure is only implemented for objects that previously used path and filename entities. For example, a file can now be expressed as either an absolute path or as a path and a filename. While the choice structure is currently only available for file-based objects it can expanded to cover other elements.

SharePoint Component Schema

A SharePoint component schema has been introduced in Draft 2 of the Version 5.6 release of the OVAL Language.

The LDAP and Service Effective Rights Tests

The LDAP and Service Effective Rights tests were introduced in Draft 2 of Version 5.6 of the OVAL Language. The LDAP test was added to the Independent component schema and the Service Effective Rights test was added to the Windows component schema.

Deprecated Items

The resolve group behavior has been deprecated in favor of using variables to reference more efficient objects for expanding groups. An example object is the sid_object.

Deprecation Policy

The Version 5.6 release of the OVAL Language will be the first release since the introduction of the deprecation policy. This release includes additional metadata that states why a particular language construct has been deprecated, and if possible, recommends a replacement construct. This release also

includes additional Schematron rules that generate warnings when a deprecated language construct is used.

OVAL Version 5.6 Discussion

Concerns Regarding the SharePoint Schema

The 'spiissettings' are all IIS-specific and not SharePoint-specific. As a result, many of these settings are available through the registry. The primary concern is that if these settings are IIS-specific it might make more sense to create an IIS component schema. More information about this topic can be found at http://n2.nabble.com/First-test-for-the-SharePoint-component-schema-tp2633049ef20093.html.

Switching from the POSIX to PCRE

The consensus from the Security Automation Conference is to switch from the POSIX regular expression syntax to the PCRE regular expression syntax. Two options for making this change are available. The first option is to change to documentation to specify that the regular expression syntax for the OVAL Language is PCRE. The second option requires the addition of a new value, 'pcre pattern match', to the OperationEnumeration type utilized by the operation 'attribute' and the deprecation of the 'pattern match' value from the OperationEnumeration type. This topic is being re-visited because there has been minimal discussion on the oval-developer-list and we feel that the topic is very important since it was originally brought up as a major version change, but is now going to be included in the release candidate of Version 5.6 of the OVAL Language which is a minor version change. A concern that has been expressed regarding this issue is whether or not the existing content will be affected. The affect on the existing content, if any, will be minimal. After reviewing different sources of OVAL content, including the OVAL Repository, Red Hat Repository, and FDCC, it appears that the content will be unaffected as it already uses the PCRE regular expression syntax.

N-Tuple Support

Adding n-tuple support to the OVAL Language is not currently in Version 5.6 of the OVAL Language because the topic raised mixed feelings among different parties at the Security Automation Conference. Some parties felt that this new capability should be developed in a sandbox environment whereas other parties felt that, if it does not break backwards compatibility, it should just be added to the OVAL Language. Also, there have not been any concrete examples that demonstrate the need for this capability. Concrete examples are very useful as they would serve as requirements for implementing this new capability. There has been some discussion on the oval-developer-list stating that there is a need for this capability, and there have been talks that the future versions of Windows operating systems (e.g. Windows 7) will require this capability. The board members were then asked if they had any concrete examples that demonstrate the need for n-tuples in the OVAL Language. Melissa Albanese stated that she may have some concrete examples, and will get back to Jon Baker, pending releasability restrictions. The second option of the proposal for adding n-tuple support will add a new structure to the OVAL Language. This element is a 'resultset' element which would allow entities to have child 'field' elements that are uniquely identified by their 'name' attribute. An important issue when considering this proposal is that this entity is very different than any other structure already present in the OVAL Language. It would also result in the creation of an oval-def:ResultSetType which could be re-used and

the new element would only have the necessary attributes thus simplifying it. On the other hand, it would result in the element being much different than any other element in the OVAL Language. The OVAL Board was then asked if there were any concerns about moving forward with this proposal. No concerns were expressed at that time.

The proposal to introduce n-tuple support in the OVAL Language raises questions as to whether or not the language should strive to be very consistent in order to facilitate learning, or, if the language should disregard some consistency in order to provide additional functionality. Another way of phrasing this question is it more important to make the schemas more readable, or, is it more important to re-use structures across different tests even though it would result in the schemas becoming less readable and more complex? One OVAL Board member said that it is not beneficial to include unnecessary attributes, elements, etc. in order to maintain consistency if it means that it would simplify the language. This notion of consistency in the OVAL Language has been a major topic of discussion internally at MITRE and we would appreciate any feedback that OVAL Board may be able to provide regarding this topic.

The OVAL Board was then asked if this capability needed to be present in Version 5.6 of the OVAL Language, or, if it could wait until the release of Version 5.7. If we were to add this capability to Version 5.6 of the OVAL Language, it would mean that the final release date would have to be pushed back, but, there would still be enough time to have it ready for the SCAP 2010 deadline. Some of the OVAL Board indicated that they were not ready to answer that question whereas other members said they would like to see it available for SCAP 2010 in September instead of waiting for SCAP 2011. It is important to note that just because Version 5.6 of the OVAL Language is ready it does not mean that SCAP 2010 would use it. It is recommended that the OVAL Board, and members of the OVAL Community, review the minutes regarding n-tuple support from the Security Automation Conference as well as the posts on the oval-developer-list and think about whether or not it should go into Version 5.6 of the OVAL Language. It is also important to think about how organizations can support this feature as well as concrete examples that can be provided as requirements for its implementation. Any proposals, comments, or questions should be posted to the oval-developer-list for further discussion. If necessary, an ad-hoc conference call can be arranged before Friday July 17, 2009 to help move things along with regards to this topic.

Final Considerations Regarding the Version 5.6 of the OVAL Language

Version 5.6 of the OVAL Language is the largest minor release to date. As a result, we are relying very heavily on the input of the OVAL Board, and the OVAL Community, in order to ensure that everyone is comfortable with these changes and that we are moving in the right direction. We would much rather know if there are any issues now instead of after Version 5.6 of the OVAL Language is released. Therefore, we are once again seeking approval from the OVAL Board before we release Version 5.6 of the OVAL Language. A proposal was made to actually have a vote on whether or not Version 5.6 of the OVAL Language would be released. Traditionally, the vote has been more of a general consensus among the OVAL Board, but, the idea of having an actual vote will be considered.

Another proposal was made to meet up during the NIST Conference and have working groups. In the past, during the NIST Conference, MITRE has done SCAP tutorials, however, as of right now, nothing else

has been planned. A few considerations regarding having working groups at the NIST Conference is that we have generally had more involved discussions before a release of the OVAL Language and what would be the basis of these discussions. It is possible that the discussions could revolve around some of the outstanding issues present in the OVAL Language. This issue will have to be considered further before a decision is made.

Actions

- MITRE will continue to work towards the Version 5.6 release of the OVAL Language on August 14, 2009.
- MITRE will schedule conference calls, and initiate discussion on the oval-developer-list, as necessary to resolve outstanding issues.
- MITRE will work towards the next build of the OVAL Interpreter for July 24, 2009.