OVAL Board Meeting (1/6/2014)

Attendees

Scott Armstrong – INADEV Corporation
Carl Banzhof – Rockport Systems
Jamie Cromer – Symantec Corporation
Blake Frantz – Center for Internet Security
Morey Haber – BeyondTrust, Inc.
Kent Landfield – McAfee, Inc.
Steven Piliero - Unified Compliance
Amaresh Shirsat – Symantec Corporation
David Solin – jOVAL.org
Randy Taylor – ThreatGuard, Inc.
Jack Vander Pol – SPAWAR, U.S. Navy
Dave Waltermire – NIST
Chris Wood – Assuria Limited

Jonathan Baker – MITRE
Matt Hansbury – MITRE
Danny Haynes – MITRE
David Rothenberg – MITRE
Luis Nunez – MITRE

Invited Guests

Melanie Cook – NIST

Meeting Summary

Welcome

The group was welcomed to the 2014 1st quarter OVAL Board Meeting.

Status Report

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

OVAL Language/Interpreter

To assist with incorporating OVAL Sandbox capabilities into an official Language release, an OVAL proposal form was developed with input from the OVAL Board. The form was covered later in the meeting.

On January 3, Version 5.10.1.6 of the OVAL Interpreter was released on SourceForge. Included in this update was an upgrade to the Xerces and Xalan libraries bundled with OVALDI. Xerces was upgraded to version 3.1.1 while Xalan was upgraded to version 1.11. Also included were numerous bug fixes requested by the community.

OVAL Repository

At the time of the call, the number of Definitions within the OVAL Repository was 18,849. There was a large increase in community participation, which resulted in four top contributors for this quarter. The OVAL Repository Top Contributor designation was awarded to ALTX-SOFT, G2 Inc., Hewlett-Packard, and SecPod Technologies.

OVAL Adoption

There were no new OVAL Adopters this quarter. Recently, the MITRE team made a small adjustment to the OVAL Adoption Questionnaire to include information about how the tool collects data from an endpoint. The team has been following up with OVAL Adopters to try and get updated questionnaires filled out with this new information. A further follow-up message is planned for OVAL Adopters who have not yet responded.

OVAL Sandbox Proposal Form Discussion

The OVAL Sandbox proposal form was created to formalize the process by which new significant features are presented to the OVAL Board. This form allows the contributor to identify a feature, provide contact information, and highlight how it benefits the Language. After an initial review of this form by the OVAL Board, an additional set of questions was added to allow for information regarding how a capability affects the Language, including its effect on tools and end users, as well as its overall technical merits. Dan Haynes led the group through some additional discussion of the form and the process around it.

After an updated version of the document was sent out to the mailing list, some Board members had additional questions and comments about the form. One of these questions was around how the Board would determine which contributions would require use of the form. During discussion of the topic, some specific examples were given to illuminate the best way forward. Additionally, some of the members that represent tool vendors made it clear that documentation updates were not always minor changes and that some would require a Board vote.

The group agreed that allowing less significant issues should not go through a vote. Examples of less significant issues include typos and documentation updates that would not require major changes in meaning of a feature. New tests or schemas, and documentation updates that result in major changes to the meaning of a feature should require a vote. The MITRE team agreed that part of the process will include notifying the Board of a proposed set of features that would and would not require votes. This will allow the Board an opportunity to review this proposed list of voting features for correctness. Additionally, the team will update the process documentation to provide rough guidelines on which types of features would need a vote.

Another comment on this form related to the Technical Review section. It was requested for question one on the form to clarify or document the accepted design conventions for the Language. The MITRE Team agreed to make this clearer. The other request was around the specific release for which a change would be targeted. It should be defined what makes the targeted release major, minor, or whether it falls under the exceptions clause. Rather than determining the exact targeted release, one Board

member suggested to instead target the type of release the change would be applicable to. Additional feedback was to rephrase a question on impact and how it allowed for new capabilities to accomplish what could not be before.

OVAL Separate Core and Platform Version Discussion

During the 2013 Q4 Board meeting the MITRE team committed to working on a proposal to separate the versions for the Core and the Platform Extension Schemas. Matt Hansbury presented for the Board an initial proposal for how this change might be executed. This proposal is a result of several conversations over the years about how versioning things separately could help alleviate a few areas of concern for the community.

In its current state, there is one version that encompasses the entire set of schemas, including both the Core schemas as well as the Platform Extension schemas. Versioning all of the schemas in a single package has had the benefit of keeping the versioning simple. In addition, this made the most efficient use of the Moderator's time.

Matt also presented several drawbacks to the current model, including the long release cycles for the Language and frequent appearance of changes to certain parts of the Language when no significant changes were made. Some members suggested that long release cycles actually proved to be a benefit as it allowed for more stable tools and language validation. It was asked of the Board whether this policy of separate versioning would help communicate to sponsors what platforms they support. The overall consensus was that it depended on how the separation was carried out, but that in general it would help.

Following the description of the current state, Matt presented a proposal designed to spark discussion on the topic with all decisions open to discussion and feedback. The central proposal was to separate the versioning of the Core schemas and all of the Platform extensions. This proposal for separating the versions included adding another identifier to the three-part current version. This would allow for the specific platforms to be tied to the current version of OVAL without ambiguity. The specific delimiter used for this fourth identifier is still to be determined, but feedback during the call suggested that using a new delimiter (that is not a period) should be considered. This was viewed as an acceptable solution by the group. Additionally the group agreed with the MITRE team that re-starting the versioning at 1.0 would be a poor idea. There was also discussion of expanding the fourth identifier to indicate major and minor revisions to the platform schemas, which was also seen as beneficial.

While this would be seen as helpful, it would additionally complicate other aspects to supporting OVAL, such as SCAP Validation. It would need to be communicated what version of each platform gets validated. As individual Platform Extensions would be revised at a quicker pace, this could cause validation issues. The solution seen for this problem would be to version everything individually, but declare a rolled-up version to be "official" with respect to SCAP efforts. This would represent a snapshot in time of what is expected for validation, and would prevent tool vendors from having to constantly update tools to maintain the latest developments. Dave Waltermire of NIST indicated that he believed that such a validation scheme would be reasonable.

Lastly, there was an open discussion to begin consideration for other factors affected by such a change. One topic brought up was how to validate against multiple platform schemas in an OVAL document. It was suggested that upon revisions, updating and using properly namespaced elements should resolve document validation. As the proposal was only recently shared with the OVAL Board, more time was required to possibly identify other issues.

Conclusion

The OVAL Board was very receptive to the idea of the separate versioning policy. This was seen as a viable method to reduce overhead resources associated with broadly updating unchanged schemas. The concern for SCAP validation was met with supporting ideas to make it work. A new proposal would be drafted and proposed to the OVAL Board for the individual platform versioning taking into account all discussions held.

Furthermore, progress was made on how to successfully migrate capabilities from the OVAL Sandbox and into an official release with the OVAL Sandbox proposal form. This form is to be distributed to the OVAL community once it has been updated to reflect all the feedback provided by the OVAL Board members. Additional clarifications would be provided where necessary to help the submitter with determining targeted releases, as well as whether it technically aligns with the existing schemas.

Action Items

1. MITRE team to update documentation around voting and contributing to the Language to include feedback from Board.
2. MITRE team to continue to document and lead discussion around the proposal to separate the schema versions.