

OVAL Board Meeting (10/20/2014)

Attendees

Scott Armstrong – INADEV Corporation
Jamie Cromer – Symantec Corporation
Blake Frantz – Center for Internet Security
Tigran Gevorgyan – Qualys, Inc.
Steve Grubb – Red Hat Inc.
Kent Landfield – McAfee, Inc.
Chandan M C – Hewlett-Packard
Adam Montville – Tripwire, Inc.
William Munyan – Center for Internet Security
Steven Piliero – Unified Compliance
David Solin – jOVAL.org
Chris Wood – Assuria Limited
Dave Waltermire – NIST
Jack Vander Pol – SPAWAR, U.S. Navy

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

Meeting Summary

Welcome

The group was welcomed to the 2014 4th quarter OVAL Board Meeting. New members Evani Prasad and Chandan M C from Hewlett-Packard, and Adam Montville from Tripwire were welcomed to the OVAL Board.

Status Report

MITRE delivered a status update of the OVAL project. The following items were covered:

OVAL Adoption

No new organizations have been recognized as an Official OVAL Adopter or made a declaration to support OVAL.

OVAL Language/Interpreter

The OVAL Board has voted on adding five new capabilities to the OVAL 5.11 release since the last Board call. These include adding and updating 3 Cisco platform schemas, adding an Apple iOS schema, adding a NETCONF schema, adding a Juniper JunOS schema, and including the Linux systemd related tests.

During some of the votes on the aforementioned features, quorum was not reached. As directed by OVAL's sponsor, these votes were considered valid because there was a clear indication one way or another on whether or not to include the new feature.

The OVAL Board currently has one open voting period for including the Solaris virtualization test. In the near future, the OVAL Board will be voting on the Windows user right test. Although not previously in scope for OVAL 5.11, new Mac OSX tests have been created that would greatly improve Mac OSX platform support. Since the existing tests are outdated, it may be beneficial to consider them for inclusion. A quick survey of the attending Board members revealed no objections to putting these Mac OSX tests out for a discussion period and vote. Another Board member requested that the Board consider adding clarifications to symlink traversal as well.

Per the sponsor's direction, MITRE is not currently doing any active development with the OVAL Interpreter. As such, there are no new changes to the OVAL Interpreter for this quarter. To ensure that the Interpreter works with the upcoming 5.11 version of OVAL, a new build will be created to provide compatibility and correct validation of the new version, but with no new features implemented. One Board member asked the question of what would happen to further development of the OVAL Interpreter in a situation where MITRE was no longer moderating the effort. MITRE is currently focused on the plan to transition the OVAL Repository and has not arrived at a transition plan for the OVAL Interpreter at this time. The optimal outcome would be for a volunteer to take ownership responsibilities for the open source reference implementation. This would likely be a simple transition since the OVAL Interpreter is already open source, and does not require the constant input that maintaining the OVAL Repository requires.

OVAL Repository

At the time of the call, the number of Definitions within the OVAL Repository was 24,389. The OVAL Repository Top Contributor designation was awarded to ALTX-SOFT, Hewlett-Packard, and SecPod Technologies for their numerous contributions.

OVAL Transition Plan

MITRE walked through a presentation that laid out a more detailed plan for the transition of the components of the OVAL project. Included in this were updates to the OVAL documentation overall, with a particular concentration on how to properly extend the Language, the plan to submit parts of the OVAL Language for inclusion in the IETF SACM WG architecture model where appropriate, and the first stages of transferring the OVAL Repository. MITRE has met with two interested parties over transferring the operation of the OVAL Repository and has shared the outcomes of these conversations with the DHS sponsor. It is expected that the sponsor will consider this feedback and make a decision on how to handle the transition in the near future.

Several questions from OVAL Board members were raised with regards to conflict of interest in the new operator of the OVAL Repository. One member representing the Center for Internet Security (CIS¹)

¹ <http://www.cisecurity.org/>

identified his organization as one of the interested parties. CIS is another non-profit organization which already maintains their own repository of OVAL content. Their plan for hosting the OVAL Repository would be to mirror what MITRE has done, but on CIS servers. No membership would be required to view or submit content. They would potentially be looking for ways to improve the process of getting content approved for inclusion into the Repository. An announcement regarding the transition of the OVAL Repository is expected by the end of November.

The improvements to the OVAL documentation would greatly assist new community members with picking up OVAL from no prior experience. For more experienced OVAL users, idioms would be created to describe different approaches to various uses of OVAL and provide real examples of tests used over the years. This will be modeled after the STIX project's <http://stixproject.github.io/> web site. The Board agreed that this approach would serve as an improvement to expanding OVAL knowledge.

Additionally, MITRE is composing several whitepapers per the direction of the DHS sponsor. These whitepapers will document how selected components of the OVAL Language would benefit the SACM architecture model. These whitepapers are part of MITRE's commitment to assisting the SACM effort.

SACM

Adam Montville provided an update of current SACM WG efforts. IETF 91 is scheduled for November in Honolulu, Hawaii. The SACM WG will be having one session on Monday and one session on Friday to allow for working sessions in between. This approach proved efficient at IETF 90. The WG currently has the architecture draft and updated requirements document. Their previous submission for the use case document has been delayed. Additionally, it is expected that an updated information model will be submitted prior to IETF 91. Adam reminded the group that SACM is still needs more individuals to get involved and provide comments over the SACM mailing list on the documents.

Separate Versioning Policy

During the 3rd quarter OVAL Board call, MITRE led some conversation on making changes to the current versioning policy. The specific changes would separate out the core and platform extension version numbers into more detailed components to allow individual revisions. There have been no negative responses to this proposal so a voting ballot for officially adopting the new policy will be submitted to the Board soon. This versioning policy will go into effect with the release of OVAL 5.11. There were no objections during the call to this approach.

Conclusion

MITRE has identified a viable timeline and strategy for transitioning away from moderation of the OVAL Repository and eventually the OVAL Language. Until the OVAL 5.11 release, MITRE and the OVAL Board will continue to expand the Language to meet current needs. New documentation is planned to serve as the launching point for future OVAL adopters in the absence of a moderator presence. The OVAL Board is encouraged to participate with the IETF SACM WG to help drive a consensus information model.

Action Items

1. MITRE to draft an updated versioning policy document for OVAL 5.11 and send it to the OVAL Board for review, discussion, and a vote.
2. MITRE to transition documentation for OVAL to a GitHub pages site.