OVAL Board Meeting (01/12/2015)

Attendees

Jamie Cromer – Symantec Corporation
Blake Frantz – Center for Internet Security
Tigran Gevorgyan – Qualys, Inc.
Steve Grubb – Red Hat Inc.
Morey Haber – BeyondTrust, Inc.
Kent Landfield – McAfee, Inc.
William Munyan – Center for Internet Security
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
Adam Montville – IETF SACM Working Group Liaison
Scott Armstrong – INADEV Corporation

Danny Haynes – MITRE
David Rothenberg – MITRE

Invited Guests

Kim Watson – DHS

Meeting Summary

Welcome

The group was welcomed to the 2015 1st quarter OVAL Board Meeting. Adam Montville was welcomed back to the OVAL Board as a liaison for the IETF SACM Working Group which is a non-voting position.

Status Report

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

OVAL Adoption

There were no new Declarations or Official OVAL Adopters for this quarter.

OVAL Language

Version 5.11 of the OVAL Language was published on December 18th, 2014. This release introduced support for several new platforms including Google Android, Apple iOS, Cisco IOS-XE, Cisco ASA, Juniper JunOS, and NETCONF as well as several new tests for Linux, Solaris, and Windows. This release also included several documentation improvements and bug fixes. A complete list of changes for the release

can be found in the changelog[1]. Along with the release, an updated version of the OVAL Versioning Policy[2], which supports separate versioning of the core and platform extension models, went into effect. Lastly, it was mentioned that two issues were discovered with the OVAL 5.11 release. The first issue involved incorrect Schematron rules in the MacOS and UNIX schemas and the second issue involved the incorrect implementation of the constructs needed to support the separate versioning policy. Given that these issues need to be fixed, one OVAL Board member asked if it would be a good time to address the updates to the linux-def:RpmVerifyFileBehaviors. It was explained how that seemed like a reasonable request, but how to proceed, would be left to the OVAL Board to decide.

OVAL Repository

At the time of the call, the number of Definitions within the OVAL Repository was 25,803. The OVAL Repository Top Contributor designation was awarded to: ALTX-SOFT, Hewlett-Packard, and SecPod Technologies.

OVAL Interpreter

There was no update for the OVAL Interpreter this quarter, however, it will need to be updated to include the OVAL 5.11 schemas and support the separate versioning policy.

OVAL Transition

A brief update on the various tasks related to transitioning knowledge about the OVAL Language to the community was given. MITRE is continuing to work on the guide for creating OVAL extensions and OVAL content. These documents aim to provide an overview of the respective processes, walk through examples, and discuss best practices. Once the first drafts of these documents are complete, they will be sent to the oval-developer-list for community review and will be updated based on subsequent feedback. MITRE is also going through documentation on the OVAL website as well as internal repositories to determine what information will be useful for the community moving forward and should be made available on GitHub. Lastly, it was also noted that there wasn't any major news on the transition of the OVAL Repository other than MITRE is currently looking into what it would take to break the OVAL Repository apart from the OVAL website.

SACM Update

Adam Montville provided an update on the progress of the IETF SACM Working Group. The IETF SACM Working Group has passed all of its milestones and is currently working to develop new milestones. A new Endpoint ID Design Team was established to tackle to the problem of endpoint identity and is working to develop a solution and provide input back into the working group. The IETF SACM Working Group is also working to determine if they should submit the Use Cases document to the IESG. They are also planning to submit the Architecture and Information Model documents to the IESG. Lastly, there is

[1] OVAL 5.11 Changelog http://oval.mitre.org/language/version5.11/changelog.txt
[2] OVAL Versioning Policy http://ovalproject.github.io/documentation/policy/versioning/

a Virtual Interim Meeting on February 9th, 2015 from 10 AM – 12 PM EST[3] and the IETF 92 Meeting is in Dallas from March 22 – 27th.

OVAL 5.11 Issues

Next, the two issues discovered in the OVAL 5.11 release were discussed in greater detail. The first issue involves incorrect Schematron rules in the MacOS and UNIX schemas[4]. In the MacOS schema, there are several Schematron rules that check to make sure an OVAL State, referenced by an OVAL Filter in an OVAL Object, is of the correct type with duplicate pattern identifiers which should be unique. In addition, some of these Schematron rules reference a macos_object which is not correct. It should be referencing the specific OVAL Object that it is checking (e.g. systemprofiler_object). In the UNIX schema, the Schematron rule that checks to make sure the OVAL Test references an OVAL State of the same type uses the experimental x-macos-def namespace instead of the unix-def namespace. The second issue with OVAL 5.11 involves the incorrect interpretation of the separate versioning policy in the oval:GeneratorType construct[5]. Specifically, it incorrectly instructs implementers to use the xmlns attribute to specify which platform a schema_version element corresponds to. This documentation should be removed and an optional "platform" attribute should be added to allow content to specify the correct platform.

After the OVAL 5.11 issues were presented, the OVAL Board was asked if there were any concerns with making these changes in accordance with the separate versioning policy or if it would represent significant challenges in their products and services. If not, this would be the best approach because it would provide an opportunity to put the separate versioning policy in action and see if there are any updates that would need to be made. If it proves to be a challenge, another approach would be to just ignore the separate versioning policy and fix everything in a 5.11.1 release. This is less than ideal given that the separate versioning policy went into effect with the release of OVAL 5.11. Several members of the OVAL Board explained how they did not see fixing the schemas using the separate versioning policy as being an issue for their products and services. Given that, MITRE will document the approach outlined on the call and send it to the oval-board-list so that the entire OVAL Board can review it and consider if it will represent any challenges for them.

List of Transition Tasks

Next, a list of transition tasks, which MITRE has traditionally performed in its moderator role, was discussed as these tasks will need to be taken over by the OVAL Board and community. Tasks on this list included reviewing proposal and proposal forms, planning and publishing releases, board governance, transferring the OVAL Repository, updating and migrating documentation to GitHub, moderating the various repositories on GitHub, and planning transition strategies for the other project components (OVAL Interpreter, OVAL Utilities, OVAL Test Content, etc.). The OVAL Board agreed that this list

---

[3] February 9th IETF SACM Virtual Interim Meeting http://www.ietf.org/mail-archive/web/sacm/current/msg02335.html

[4] Incorrect Schematron Rules Bug https://github.com/OVALProject/Language/issues/235

[5] Incorrect Implementation of the Separate Versioning Policy in the oval:GeneratorType Construct https://github.com/OVALProject/Language/issues/236

seemed fairly complete and requested that it be sent out to the oval-board-list for further review. It was also stressed that some of these tasks (i.e. determining a board governance model) will take time and will need to started right away to make sure we get them taken care of prior to the end of July. One member suggested that there may be value in establishing a team or organization to take the lead on some of these transition tasks. Several members of the OVAL Board agreed and some even volunteered to help with some of these transition tasks. Lastly, a member suggested that a follow up OVAL Board call should be held to discuss the potential governance models for the OVAL Board.

Action Items

- MITRE to schedule a follow up OVAL Board call on January 26th, 2015 to further discuss the governance of OVAL.
- MITRE to prepare a spreadsheet comparing the governance models of the IEEE, IETF, and TCG.
- MITRE to document the approach for addressing the issues in the OVAL 5.11 release and send it to the OVAL Board for further discussion and to ensure it does not negatively affect any products or services.