OVAL Board Meeting (7/14/2014)

Attendees

Melanie Cook – NIST
Blake Frantz – Center for Internet Security
Rosario Gangemi – IBM Corporation
Tigran Gevorgyan – Qualys, Inc.
Morey Haber – BeyondTrust, 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

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

Invited Guests

Kim Watson – DHS

Meeting Summary

Welcome

The group was welcomed to the 2014 3rd quarter OVAL Board Meeting. Melanie Cook from NIST and Panos Kampanakis from Cisco were welcomed to the OVAL Board.

Status Report

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

Project/Funding/Other (Kim)

MITRE presented an update to the OVAL Board regarding the funding for the OVAL project. Recent funding concerns has forced an accelerated schedule for the remaining items to be voted upon for inclusion into the OVAL 5.11 release. These votes are targeted to be resolved by the end of July. With this change in mind, MITRE will more highly prioritize the transition strategy over other project efforts such as OVAL Interpreter development and OVAL Repository maintenance.

OVAL Language/Interpreter

The OVAL Board has successfully voted on adding three new capabilities to the OVAL 5.11 release. New tests include Solaris IPS and SMF configuration assessments, the license_test for Windows based platforms, as well as the new Android platform. The Android platform is based on generic Android but has the potential for additional vendor-specific features to be included in the future.

Over the next few weeks, there will be a more rapid pace to the voting process on issues previously discussed. Some of the tests yet to be voted upon include the system_test, ini_test, Cisco IOS updates, userrights_test, and the sql511_test. In addition, several new platforms under consideration include Apple's iOS, Cisco's IOS-XE and ASA, NETCONF, and Juniper JunOS.

Lastly, the Board has already been notified for three new Board prospects. These three individuals include Evani Prasad (Hewlett-Packard), Chandan M C (Hewlett-Packard) who has been active with the OVAL Repository, and Adam Montville (Tripwire Inc.) who is a former Board member.

The OVAL Interpreter reference implementation has not seen a new official release, but still benefits from several improvements. Four new probes have been implemented for the Mac platform. Additionally, multiple bug fixes brings the Interpreter into a greater alignment with the OVAL Specification. The new probes and bug fixes will be available in the next release.

OVAL Repository

At the time of the call, the number of Definitions within the OVAL Repository was 22,638. The OVAL Repository Top Contributor designation was awarded to ALTX-SOFT, Hewlett-Packard, and SecPod Technologies for their numerous contributions.

OVAL Adoption

Official OVAL Adopters

- Tripwire for their Tripwire Enterprise product

Declarations

- New Net Technologies for their NNT Change Tracker Enterprise product

SACM Information Model

Dave Waltermire of NIST and Kim Watson of DHS submitted an informational model draft to the SACM working group on July 3rd. This informational model draft covers topics of managing endpoints, software, configurations, and vulnerabilities. The model outlines the problem scope, required elements, discusses related work, and documents what needs to be done. Kim would like to include this work within DHS's CDM program and therefore hopes that by continuing to grow this work out of existing efforts there will not be a pause in progress.

Open questions that remain for MITRE and the Board relate to usage of the OVAL Repository and whether it meets the needs of the community. She envisioned a situation where MITRE will no longer be paid to process content submissions and instead transition the Repository to an interested party within the next three months. To address other concerns, Kim encouraged others to attend related workshops and IETF meetings to provide industry perspective. Proper representation is of the utmost importance. Also announced was the Security Automation workshop in MITRE McLean on August 26-28.

One OVAL Board member asked about the drivers that prompted Dave Waltermire and Kim Watson to submit the information model to the IETF. Dave explained how his primary driver was to get the business requirements and relate them back to the SACM use cases. Kim explained how her primary driver was to develop something that could be used from the abstract concepts that have been discussed in the SACM WG to identify what is needed, processes, and addressing interoperability challenges building off the communities 10+ years of experience so that they do not have to start from scratch.

Dave also expressed how he saw the SACM Information Model for Endpoint Assessment as complementary to SACM Information Model Based on Trusted Network Connect (TNC) where the Endpoint Assessment model focuses more on data formats and the TNC model focuses more on data exchange and interoperability.

Unofficial Extensions in OVAL

Following the 1st quarter OVAL Board call, MITRE spent time revising the concept of separating the versioning of the core and platform extension schemas. An email detailing the new plan was sent to the OVAL Board and took into consideration all feedback provided by Board members. As the versioning policy is currently defined, there is one version for the Language as a whole. This becomes an issue when much of the core schemas remain consistent while platforms undergo changes more frequently. It also complicated claims of support when one version tied together all platform extensions.

The new proposal will utilize two version identifiers to track advancements in the Language. One version identifier will represent the core schemas and elements, while a second version identifier will represent the individual platform extensions. One suggestion taken from the 1st quarter Board call was to prefix the platform version values with the core version value. Similar to the current practice, there would be a major, minor, and optional update portion for both core and platform identifiers. As an example, one would see a version similar to Windows 5.11.0:1.0" for a platform version rather than "Windows 5.11". Bundles of core and platform extensions would be optionally provided, outside of OVAL, in a "rolled up" package to contain a snapshot in time for purposes such as SCAP Validation testing. One OVAL Board member explained how they like the level of granularity presented in the proposal.

The concept for what was defined as core schema and what fell into platform extensions was outlined in the appendices of the proposal document. There was a minor debate about the inclusion datatypes in the core versus in the platform extensions. This needs to be examined further as datatypes transcend platforms extensions as the ind-def:variable_test allows for the use of all datatypes.

One Board member raised the question of future impacts for such a proposal, wondering how it would affect content maintenance. It would not be ideal to modify content every version change. MITRE noted that the core does not often change and thus would be likely limited to platform revisions. There are methods that exist to ensure that content being offered is done so at the minimally supported schema version to maximize support. This principle of least versioning, currently implemented in the Repository would apply towards platform extension versions in a similar manner. The same Board member also raised a point of interest in trying to foster a community-led maintenance effort of the new platforms.

All Board members on the call felt it would be appropriate to implement this process change beginning with OVAL 5.11, although a consensus would be requested from the remainder of the Board over the oval-board-list.

Next, MITRE opened discussion on the current documents that discuss how to develop new proposal and extend OVAL. This focused on two documents that outline how to make a change to the OVAL Language. One document[1] states what would be expected when a user wishes to create a new Test or update an existing one, and what sort of documentation should accompany the request. However, this documents fail to capture how or why OVAL elements were designed in such a way. The other document[2] covers the extensibility of various constructs in the OVAL data models, yet without explaining why one may wish to do so. It is MITRE's goal to update these documents to better cover the design decisions and best practices that should be considered when extending the OVAL Language. As more and more of the OVAL project is transitioned to the community, this documentation will become more critical as the community will primarily be responsible for developing and vetting the extensions that they need.

Conclusion

MITRE has specific goals and deadlines to drive forward transitions of the OVAL Language and OVAL Repository. To better help the community, Board members were encouraged to become more involved in IETF SACM work and attend related workshops. Board members should expect minor changes in the near future with existing processes to aid in an accelerated schedule of making sure the release of OVAL 5.11 covers the needs of the community.

Action Items

1. MITRE to email OVAL Board for consensus of beginning new versioning policy with OVAL 5.11.
2. MITRE to update documentation on extending the OVAL Language.

[1] http://oval.mitre.org/language/about/change_requests.html

[2] http://oval.mitre.org/language/version5.10.1/OVAL_Language_Specification_01-20-2012.pdf - Appendix A (Extension Points within the OVAL Definitions Model)