OVAL Board Meeting (04/08/2013)

Attendees

Scott Armstrong – Symantec Corporation
Carl Banzhof – Rockport Systems
Blake Frantz – Center for Internet Security
Steve Grubb – Red Hat Inc.
Rob Hollis – ThreatGuard, Inc.
Tim Keanini – nCircle Network Security, Inc.
Kent Landfield – McAfee, Inc.
William Munyan – Center for Internet Security
Steven Piliero – Unified Compliance
Amaresh Shirsat – Symantec Corporation
Randy Taylor – ThreatGuard, Inc.
Eric Walker - IBM Corp.
Dave Waltermire – NIST

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

Meeting Summary

Welcome

The group was welcomed to the 2013 2nd quarter OVAL Board Meeting.

Status Report

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

OVAL Adoption

- ATM Software Sp. z o.o. submitted a declaration to support OVAL for their ATM Information Security Workflow product.
- Institute for Information Industry – CyberTrust Technology Institute submitted their Adoption Questionnaire and have been recognized as an Official OVAL Adopter.

OVAL Repository

An update on the status of the OVAL Repository was provided. The OVAL Repository's definition count at the time of the call was 14,524 definitions. This quarter's top contributors were ALTX-SOFT, G2, Inc. and SecPod Technologies.

OVAL Language & Interpreter

The OVAL team pushed the OVAL Language and related trackers to GitHub. This will allow the OVAL Community to add, follow, and comment on issues being tracked in the schemas. Coinciding with this was the release of OVAL 5.11 Draft 1 on February 20, 2013.

This first draft of the 5.11 version of the OVAL Language includes adding support for notes in variables, supporting collection of hives in the Windows registry probe, deprecation of Linux rpmverifypackage digest_check_passed and signature_check_passed entities, and overall improvements to documentation in the Specification and OVAL schemas. Additional capabilities and fixes will be added to future drafts.

The MITRE team is planning a release of the OVAL Interpreter next week on 4/17/13. The major change in this revision is the inclusion of IPv6 support and a couple of bug fixes on Windows and Linux. This release will be OVAL Interpreter version 5.10.1.5.

OVAL 5.11

An overview of the planned features and their status for OVAL 5.11 was presented to the Board. This included the release timeline and a more detailed overview of the different release goals. In February, MITRE released Draft 1 of OVAL 5.11, which was a relatively small draft of mostly Language clarifications and fixes. A second draft of the 5.11 Language is due out on May 8, 2013. The team is planning to produce a Release Candidate for 5.11 in July 2013 followed by an official OVAL 5.11 Language release in September 2013. Within this timeline, the MITRE Team announced that they would like to host a Developer Days event prior to the official release.

The main goals of the OVAL 5.11 release include increasing support for Cisco and Juniper network devices, adding support for Android mobile devices, ensuring support exists to allow Apple Security Guides and DISA STIGs to be fully automated, redesigning the sql_test to alleviate security concerns, addressing file system searching and performance concerns, and adding support for complex file formats.

Towards this first goal, Cisco has provided updates to the IOS schema as well as submitted new ASA and IOS XE schemas to the OVAL Sandbox. For other forms of network devices, jOVAL, SecPod Technologies, and Apex Assurance Group, have jointly submitted a preliminary Juniper JunOS experimental schema and NETCONF experimental schema to the sandbox and implemented support for both in the jOVAL engine. It was noted that Juniper is not supporting this directly but that MITRE is currently working to engage with them on this effort.

Android support for mobile devices has had significant work performed, as well. An initial schema provided by SecPod Technologies was further revised and expanded. The new version remains in the OVAL Sandbox, now accompanied by a sample OVAL Systems Characteristics producer application for Android devices. The output from this program may be exported to another system for analysis. The OVAL Team is currently looking to engage Google and other primary source mobile device vendors.

Increased support for Apple Devices involves additional capabilities for OSX that includes checking packages and improving the plist_test. These combined efforts should close some gaps found in the Apple Security Guides and DISA STIGs. It will not necessarily cover content generation. There is also a goal to add support for Apple's iOS devices. NSA created a security guide that utilized the existing Mac OS plist_test. The OVAL Team is currently looking at querying Apple MDM Servers for additional information. A Board member questioned whether we were working with Apple through their SCAP-on-Apple project. MITRE is currently looking to coordinate with Apple on these efforts.

Better support for databases was another goal for the OVAL 5.11 release. The OVAL Team has added support for a draft of the sql511_test, with no changes yet from the existing sql57_test, on a branch of the

OVAL Interpreter. This is intended to provide a test bed for the Community to evaluate the current test as well as provide a place to address new functionality and security issues that have been raised in the past. It has been made clear by the OVAL Board members that the existing method that passes credentials in clear text has been a major issue that blocks implementation.

The OVAL Team also wishes to update the current file system search and evaluation limitations. This goal includes documentation updates, support for symbolic links, and issues with treating paths as strings. Some areas of investigation include what types of normalizations may be applied to a file path, as well as the representation format. Additionally, the team hopes to optimize regular expression evaluation.

Currently, complex file types are not well supported by OVAL, and subsequently several proposals have been made to add support for common file formats such as INI, Apache configuration, and SMB configuration files. CIS has recently submitted to the OVAL Sandbox a schema for collection of INI files, and with SecPod Technologies' assistance, a patch for OVALDI to include support. They are expected to submit sample content soon.

Further sections of the OVAL Language to be addressed in 5.11 include updates to the core of the OVAL Language. This will cover items brought into discussion recently such as entity evaluation, entity casting, how to assign status values, and evaluation of deprecated constructs. This Core Language update could also include new OVAL functions.

Several additional proposals for OVAL 5.11 have been made, including support for the new Solaris 11 Image Packaging System and Service Management Facility constructs as proposed by the Oracle team. Additional candidates for inclusion include the Windows license_test and systemmetrics_test which are currently located in the OVAL Sandbox and have been implemented in jOVAL. Lastly, the scripting capability and the OVAL for artifact hunting use case require additional investigation to determine viability for inclusion in the 5.11 release.

The OVAL Team has asked the Board to help identify mature capabilities in the OVAL Sandbox so that they may be pulled into the planned release. As previously outlined in the Sandbox process, a proposal needs community review before inclusion, but as of yet, little community review has been completed. The MITRE team asked if the current process by which Sandbox contributions are promoted to the official Language makes sense and recognized that it may need to change as it is used in practice. The Board voiced its strong opinion that extensions should not be added straight to OVAL without a process in place to identify such extensions as optional to Validation programs. Furthermore, one Board member raised the point that some vendors have no interest in implementing certain extensions. This situation is further complicated by the Validation effort which may set requirements for implementations not expected from OVAL Adopters. It remains to be figured out what would be considered required in OVAL and what would be optional in this sense. Some Board members also suggested that implementations of such extensions were to be mandatory, while other Board members countered that while nice in theory, the existing Language was built without this approach. The OVAL Team will make a point to investigate these points and come up with some options.

SACM & RSA Updates

Kent Landfield was asked to provide an update of the SACM Birds of a Feather (BOF) that recently took place in Orlando in March. This was the final BOF for forming a working group. The final charter was being worked on over the SACM mailing list, with a few drafts presented. Overall, the BOF was productive and had good participation by both old and new participants. Takeaways from this meeting were changes to the charter which have already been made.

Next, Matt Hansbury gave a brief recap of the OVAL Board Face-To-Face meeting. This meeting coincided with RSA and was likewise fairly well attended. A brief history of OVAL was covered and then led to further discussion of how the Board members felt about a potential transfer of the OVAL Language to an international standards body. The Board encouraged MITRE to participate in the working group and to create an informational draft to socialize OVAL within the IETF. MITRE is working on this document, and will submit to the IETF after an internal review, including the DHS sponsor.

Board Requirements and Responsibilities

Danny Haynes introduced two draft documents intended to formalize several aspects of the OVAL Board. The first document covers processes for adding, transferring, and removing Board members. The second document covers the expected roles, tasks, and qualifications for individual Board members. These documents were based off existing OVAL Board documentation and the CVE Editorial Board requirements.

Within the roles and qualifications document, it was proposed that the Board introduce an Emeritus status to recognize former members that have made significant contributions to OVAL and allow them to remain involved with OVAL even after they have left the Board. The roles document also covered expected levels of engagement within the Board and Community.

The processes document proposed an approach for how new Board members would be added and how membership would be transferred and removed. It was based on the process for adding new members to the CVE Editorial Board. The group was given an overview of this process and given an opportunity for feedback.

Discussion

Several Board members voiced their support of implementing the new Emeritus status. There was some confusion about wording within the document that implied Board members were individually identified as a “Technical”, “Liaison”, or “Advocate” member. While companies could have three different people in those roles, only two are allowed seats on the Board. The MITRE Team accepted that some softening of the language in the document was needed to clarity that these roles were designed to describe the types of activities that a Board member could pursue, but not mandate that each organization have one person filling each role described. It was also recommended that things like ‘must’ and ‘shall’ would be better stated as ‘expected’ actions.

Another Board member wanted clarification on what these drafts were intended to address. It had been MITRE’s goal over the years to come up with better documentation for the roles and responsibilities for the OVAL Board. Since formal requirements were never established, this development could help emphasize maturity of the project. This better expresses the expectations for each Board member and provides better process on how to deal with Board members who are no longer active in their role as they once were.

Lastly, it was not clear in the proposed documents what decisional authority the OVAL Board actually held as members. The MITRE team agreed that the influence provided each Board member wasn't made clear in the documents and agreed to revisit this point.

Action Items

- MITRE to re-word the roles document to clarify that members are not uniquely identified under a specific grouping of expected tasks.
- MITRE to create an official branch of OVALDI to host the Sandbox INI file collection effort.
- MITRE to organize a follow-up call with the OVAL Board to investigate how to specify which OVAL extensions are to be included in future releases and to discuss what the expected authority of the OVAL Board is.