OVAL Board Meeting (1/9/2012)

Attendees

Eric Walker – IBM Corporation
Kent Landfield – McAfee, Inc.
Chandrashekhar B – SecPod Technologies
Randy Taylor – ThreatGuard, Inc.
Chris Wood – Assuria Limited
Carl Banzhof – Rockport Systems
Anthony Busciglio – Cisco Systems, Inc.
Aharon Chernin – DTCC
Mark Cox – Red Hat, Inc.
Christopher Johnson – Hewlett-Packard Development Company, L.P.
Dennis Moreau – RSA Security
Omar Santos – Cisco Systems, Inc.
Blake Frantz – Center for Internet Security
Jonathan Frazier – Symantec Corporation

Jonathan Baker – MITRE
Matt Hansbury – MITRE
Danny Haynes - MITRE

Meeting Summary

Welcome

The group was welcomed to the 2012 1st quarter OVAL Board Meeting and Anthony Busciglio and Omar Santos were welcomed as new members of the OVAL Board.

Status Report

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

OVAL Language/Interpreter

Version 5.10.1 the OVAL Language will become official this week. This version fixes a small, but critical bug in the 5.10 release, where the linux-def:rpmverifypackage_state is missing an entity (extended_name) that is critical to the utility of the test. This update release takes advantage of the recently modified OVAL Language Versioning Policy which now defines a third level of versioning for the OVAL Language. This allows minor updates to the OVAL Language that do not introduce new capabilities, but rather fix critical bugs. The official Versioning Policy has been updated on the website and sent out to the oval-developer-list, and contains all of the details for the policy.

During the 5.10.1 discussion, it was asked if the 5.10.1 version of the Language would find its way into SCAP 1.2. The MITRE team believes that while the SCAP specification (NIST SP 800-126) itself will continue to reference only the major and minor versions (e.g. 5.10), the SCAP Validation Program Test

Requirements (NIST IR 7511 Rev.3), will specify the version all the way out to the newly defined third version level (e.g. 5.10.1).

Since the last Board call, the OVAL team has begun working on the concept document for the Sandbox, which will be a way to allow for experimentation with the OVAL Language outside of the normal release cycle. Detailed conversation on this topic took place later in the call. Additionally, the team has sent out an initial, partial draft of the Windows Component Model Specification for comments, welcoming any feedback on both the content and style for this document. Additional updates to the Windows Component Model Specification and other Component Model Specifications will be developed and sent out over time.

The OVAL Interpreter will have an updated release, at the end of the week, incorporating some bug fixes and updates relating to the OVAL 5.10.1 Language release.

OVAL Repository

The OVAL Repository's definition count at the time of the call was 12,783 definitions. Additionally, it was announced that SecPod Technologies, DTCC, G2, Inc., and Symantec Corporation earned Q4 Top Contributor Awards for their submissions to the OVAL Repository.

Lastly, the OVAL team is preparing a survey in an attempt to collect information regarding the creation of OVAL content and the challenges therein. The team would welcome any and all feedback regarding this topic to understand how best to help content developers more easily and efficiently create OVAL content.

OVAL Adoption

With the RSA Conference 2012 coming up in late February/early March, it was suggested that vendors make sure that their information is up to date and accurate on the OVAL Adoption site. Any updates can be passed on to the OVAL team for inclusion ahead of the conference.

OVAL Sandbox Discussion

During the call, the OVAL Sandbox concept was discussed in detail. The idea of this feature is to allow the community to create and collaborate on capabilities in the OVAL Language without having to add the features to the official Language. The team highlighted the fact that most future changes would be first added to the Sandbox before adding them to the official OVAL Language, which should increase the quality of the accepted features.

Additionally, it was highlighted that the ability to pick and choose which features were implemented by a specific tool or vendor would be critical to the success of the Sandbox. It is this requirement that will drive the team to move to OVAL Schema files out to a public source control system of some sort, which will provide ways to branch the different capabilities. The group responded positively to the idea of moving the OVAL Schema files off of the static website and into a publicly accessible source control system.

The expected overall process for the Sandbox was discussed as well. The concept is still under discussion, but some features that will be supported include:

- Adding new tests to the Sandbox
- Updating tests in the Sandbox
- Removing changes made in the Sandbox
- Moving changes from the Sandbox to the official OVAL Language
- Picking and choosing which changes are desired out of the Sandbox

It was asked how the changes would be submitted to the Sandbox and also how the changes would be managed. Both of these topics are still up for discussion. Several possible methods for submitting changes were mentioned, including email, as well as a public source control system, such as SourceForge.net. It was pointed out that email is difficult to use for such a task, and in general, the community seems to prefer a source control system. It was also suggested that something like github should be considered as well, to best provide the required capabilities.

During the conversation it was asked of the vendors if they currently implement their own proprietary changes to the OVAL Language. Two vendors replied in the positive, generally doing this only in the case that they have a specific need that isn't addressed currently. The features added are generally then funneled back into the official OVAL Language over time. This seems consistent with the concept of an OVAL Sandbox.

Additionally, it was asked if the MITRE team expects to be able to implement the Sandbox changes in the OVAL Interpreter. While the OVAL team is unable to commit to necessarily implementing every change in the OVAL Interpreter, they will attempt to implement changes as appropriate. The team also reminded the group that the OVAL Interpreter is publically available code, and can be downloaded and modified by other parties.

The community had a favorable response to the OVAL Sandbox proposal, though in order to fully understand and support the concept, more details regarding the process, procedures, and implementation are required. The OVAL team is committed to providing those details.

Conclusion

At the end of the call, the OVAL team thanked the group for their time and feedback. An invitation was also given to the group to stop by the MITRE Making Security Measurable booth at the RSA Conference, for those that attend. The group was also reminded that there was an upcoming teleconference call on January 19th at 2 PM to discuss the versioning policies of the various SCAP languages and might be of interest given the recent OVAL Language Version Policy discussions. Lastly, it was mentioned that the MITRE team is working with NIST on scheduling developer events for early/mid 2012. A notional schedule would include an event hosted by NIST in Maryland in April, and an event hosted by MITRE in Bedford in early July.