OVAL Board Meeting (01/11/2010)

Attendees

Jonathan Baker – MITRE
Danny Haynes – MITRE
Mike Lah – MITRE
Jasen Jacobsen – MITRE
Allison Ounanian – MITRE

Blake Frantz – Center for Internet Security (CIS)
Melissa Albanese – DoD
Pai Peng – Hewlett Packard
Jay Graver – nCircle Network Security, Inc.
Alex Quilter – nCircle Network Security, Inc.
Chris Johnson – NIST
Dennis Moreau – RSA
Chandrashekhar B – SecPod Technologies
Rob Hollis – ThreatGuard, Inc.

Meeting Summary

Welcome

The group was welcomed and thanked for attending the 1st quarter 2010 OVAL Board Meeting.

Status Update

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

- OVAL Language
  - The team has been reviewing the Schematron rules for the OVAL Language in order to optimize them and reduce the time it takes to validate an OVAL Document.
  - The notion of OVAL Reporting has been introduced to the OVAL Community over the oval-developer-list.
- OVAL Interpreter
  - ovaldi-5.6.4 was released on January 6, 2010.
  - Support for the unix-def:inetd_test, unix-def:xinetd_test, win-def:metabase_test, and ind-def:ldap_test have been added.
  - Support for the filepath entity has been added.
  - The ind-def:filemd5_test and ind-def:filehash_test were rewritten to use OpenSSL library.
  - Support for the SHA-1 entity has been added.
  - The location of ovaldi.log file can now be specified with the '-y' command line option.

    - The OVAL Interpreter now uses the OpenSSL library on Windows and the OpenSSL and OpenLDAP libraries on Linux.
    - We will begin to work on the Solaris and Mac ports.
- OVAL Repository
    - There have been a lot of repository submissions on the oval-discussion-list.
    - The breadth of content is diversifying. We now have all of the Debian advisories for 2008 and 2009.
    - The "Top Contributors" this quarter were DTCC, Gideon Technologies, Inc., Hewlett-Packard, NIST, and SecPod Technologies.
    - As submissions have ramped up, we have had issues handling the larger volume of content. As we move along, we will continue to improve the submission process to ensure that content is added to the OVAL Repository in a timely manner.
- Miscellaneous
    - We are planning to go to the RSA Conference (March 1-5, 2010) and we will have the Making Security Measurable booth. We currently have no vendor coordination plans beyond the standard booth presence and we speak OVAL, CVE, etc. signs.
    - The OVAL website will be refreshed soon and its look and feel will be aligned with the CVE site.
    - We are continuing to expand the OVAL Language and along the way new use cases have arisen. Originally, the OVAL Language was used to check for a specific machine state. Now there are ideas of using it in the threat and malware detection spaces. We are excited to see that people are running with the OVAL Language and applying it to new use cases.
    - Melissa Albanese – Currently, all of the checks in the OVAL Language are in user-land. Has anyone thought about kernel-land checks? Jon Baker – At MITRE, a research proposal is being developed for OVAL Attestation and using the OVAL on a trusted computing platform. However, we do not know about using OVAL Definitions for device drivers, but, we would be very interested in talking about it. Melissa Albanese - Are vendors looking into this area and would it be a big change? I guess that all of the OVAL checks are user-land checks.

OVAL Release Timeline

On January 8, 2010, an email was sent to the oval-board-list explaining how the timeline set back in October of 2009 is no longer reasonable. As a result, we need to re-evaluate our previous timeline. We have also noticed a surge in feature requests for the OVAL Language which is a testament to its increased operational use and the additional support of OVAL Language constructs in the OVAL Interpreter. The new timeline for Version 5.7 of the OVAL Language can be seen below.

- Planning – August 28, 2009
- Draft 1 – February 3, 2010
- Release Candidate – March 10, 2010
- Official Release – April 14, 2010

The Version 5.7 release of the OVAL Language will be much smaller than Version 5.6 and will focus on correcting schema issues, clarifying documentation, and the addition of a test to examine the DNS cache on both the Windows and UNIX platforms. The timeline for Version 5.8 of the OVAL Language has also been updated and can be seen below.

- Planning – Now
- Draft 1 – May 5, 2010
- Release Candidate – July 7, 2010
- Official Release – August 4, 2010

This updated timeline will provide additional time for vendors to implement the changes in Version 5.8 of the OVAL Language assuming that NIST selects it for SCAP. Jon Baker – Does this timeline seem reasonable? The OVAL Board did not express any objections to the proposed timeline and was encouraged to voice any comments that they had, or alternatively, post them to the oval-board-list.

OVAL Adoption Program Update

The OVAL Adoption Program is on the cusp of sending out invitations for OVAL Adoption Declarations. A brief overview of the program, documentation on the updated and emerging uses cases of the OVAL Language, and the mapping of these use cases to test cases in the NIST OVAL Validation Program will be provided as soon as possible. We plan to have all of the use cases completed by the end of the month. We will also release a draft of the OVAL Validation DTR, which will be limited in scope, unlike the SCAP Validation DTR. We would appreciate any feedback that you have on it. It is also very important that we get this right as a lot of procurements will depend on the OVAL Validation Program.

Rob Hollis – Will vendors have to go through a separate validation program for OVAL now? Jon Baker – The SCAP Validation Program only updates on its specified lifecycle whereas the OVAL Validation Program will advance with the language. As a result, the OVAL Language and the OVAL Validation Program may not necessarily be in sync with the SCAP Validation Program. The major advantage to this approach is that a vendor's product can be validated for support that they have added above and beyond the version of the OVAL Language specified in the SCAP Validation Program. Rob Hollis – Would OVAL Validation be done in incremental releases? Jon Baker – Yes, we would like to do this on minor releases so that vendors can keep up with the progress of the OVAL Language.

For the RSA Conference, we would like to have a complete OVAL Adoption website with the updated uses cases, the OVAL Validation DTR, and a complete list of the organizations that support the OVAL Language. We will send out a call for OVAL Adoption Declarations to the oval-board-list and make any changes necessary as a result of the diverse representation of products on the OVAL Board. We will then send out a call for OVAL Adoption Declarations, to the broader OVAL Community, on the oval-developer-list. This will be followed up by sending out questionnaires to the various organizations for completion. Having a diverse collection of vendors on the OVAL website will highlight the importance of the work on their products and the OVAL Language.

Rob Hollis – Will OVAL Validation certification expire on a yearly timeline like SCAP? Or, will it expire per version? Jon Baker – OVAL Validation is dependent on the release of the OVAL Language; however, we are not exactly sure how this should be handled. NIST may be able to provide some insight on this. Chris Johnson – We can post more information to the oval-board-list regarding the length of time that the OVAL Validation certification will last.

OVAL Reporting

We also wanted to give an update on our work with OVAL Reporting. Charles Schmidt sent an email to the oval-developer-list last week that included an OVAL Reporting RFC. The email, and RFC, can be found at the following link.

http://n2.nabble.com/OVAL-Reporting-formerly-OCRL-request-for-comments-tp4256104ef20093.html

OVAL Reporting is a light-weight addition to the OVAL Language that wraps OVAL objects with metadata and defines how these objects will be used to generate an OVAL System Characteristics document which will then be formatted by XSLT. It is also possible that an existing OVAL System Characteristics document could be referenced rather than generating one on the fly. Originally, we thought of creating our own reporting language (OCRL - Open Checklist Reporting Language); however, it seemed that no matter what we would include in OCRL, it would not be enough to satisfy the users. Therefore, we decided that XSLT would be the best way to implement OVAL Reporting. OVAL Report documents will include a section with OVAL objects and a section with XSLT that will be applied to the OVAL objects to generate the actual report.

Jon Baker – Would this be easy to implement? Does this implementation present any challenges? Are there any questions regarding OVAL Reporting? The OVAL Board did not express any concerns.

With that, the OVAL Board was encouraged to take a look at the OVAL Reporting thread and think about what it would mean for their products and organizations and to provide feedback as necessary.

Other Issues / Questions

If any members of the OVAL Board are interested, there are plans for a February 2010 Developer Days Workshop for CPE, XCCDF, and Remediation at NIST.

Jon Baker – Were there any topics that were not discussed that you would like to bring up? Or, are there any topics that require further discussion? No additional topics were brought up and the meeting concluded.

Actions

- MITRE will publish the OVAL Language release timeline, for Version 5.7 and 5.8, as soon as possible.
- MITRE will send out a draft of the OVAL Validation Program DTR to the oval-board-list.
- MITRE will send out a call for OVAL Adoption Declarations so that a complete list of organizations, that support the OVAL Language, will be ready for the RSA Conference in March.