OVAL Board Meeting (1/10/2011)

Attendees

Chris Wood – Assuria Limited
Eric Walker – BigFix Inc.
Steven Piliero – Center for Internet Security (CIS)
Luis Nunez – CISCO
Melissa Albanese – DoD
Aharon Chernin – DTCC
Morey Haber – EEYE
Todd Dolinsky – Hewlett Packard
Dave Waltermire – NIST
Carl Banzhof – Rockport Systems
Kent Landfield – McAfee, Inc.
Steve Grubb – Red Hat
Chandrashekhar B – SecPod Technologies
Rob Hollis – ThreatGuard, Inc.
Alberto Bastos – Modulo
Blake Frantz – Center for Internet Security
Jonathan Frazier – Symantec Corporation
Dennis Moreau – RSA Security
Michael Tan – Microsoft Corporation

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

Meeting Summary

Welcome

The group was welcomed to the 2011 1st quarter OVAL Board Meeting. A new member, Alberto Bastos of Modulo, was welcomed to the OVAL Board.

Status Report

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

OVAL Language

It was announced that due to a validation issue with the 5.8 OVAL Language Schema, an updated version is being drafted and released in the near future. This proposed version would be 5.9, and will be very limited, including only the fix for the validation issue. More details were provided later in the call.

OVAL Repository

The OVAL Repository's definition count at the time of the call was 10,441 definitions. The MITRE team is working on adding features to the Repository's tools to allow more efficient and accurate processing of

submissions. This work will be completed in the next few weeks. Once complete, the team will review the next set of tasks, including a fix for a much discussed "least version" for the Repository content.

OVAL Interpreter

The OVAL Interpreter team has completed support for the Microsoft SharePoint schema. It has also added support for the sol-def:isainfo_test and is currently adding support for the sol-def:patch54_test.

Additionally, there has been research on how to correctly deal with running the OVAL Interpreter on 64-bit Windows due to registry and file system redirection. On 64-bit Windows, portions of the registry and file system are separated into two distinct logical views: one for 32-bit applications and another for 64-bit applications. Any calls are then redirected to the appropriate view depending on if the application, making the call, is a 32-bit or 64-bit application. As a result, the 32-bit OVAL Interpreter cannot view information in the 64-bit view. Several proposals have been made, and they will be presented on the oval-developer-list where discussion can continue and it can be determined how best to proceed.

Lastly, due to licensing issues, research has also been undertaken to determine the most appropriate crypto library to use for the OVAL Interpreter. We have recently looked into the Crypto++ Library (http://www.cryptopp.com/) and determined that it could work as an alternative to OpenSSL and Libgcrypt. However, we have not yet decided what the best solution will be for the OVAL Interpreter moving forward.

OVAL Adoption

The Adoption program currently has 22 organizations and 30 products that have completed OVAL Adoption declarations. Additionally, there are now 5 additional repositories of OVAL content linked from the Repository web page, all of which are hosted by companies that have participated in the OVAL Adoption Program and provide a set of definitions to the public.

Also, there will be a MITRE-hosted Developer Days the week of June 14th at the MITRE Bedford site.

OVAL Language Specification Status

Since the IT Security Automation Conference, the OVAL team at MITRE has been working on developing a specification for the OVAL Language. The progress so far includes re-factoring the use cases that are currently found on the web site to better describe the cases for which OVAL is relevant. Also, the OVAL Language requirements have been reworked to reflect the updates in the use cases and expanded. Lastly, work has begun on the data model part of the specification.

Upon completion of the initial draft of the OVAL Language Specification, it will be sent out to the community for comment. Once this specification is complete, it will make it easier for individuals interested in learning about OVAL to begin their discovery of the language. Additionally, it will allow the OVAL team to better communicate how the language is built.

Release Planning

During this part of the call two future releases were discussed and rough timelines were outlined.

Release 5.9

As briefly mentioned at the top of the call, there has been an ongoing issue brought up by several folks in the community regarding the difficulty in validating the current OVAL 5.8 Schema with certain XML tools. The MITRE team verified this issue both internally, and by communicating with a 3rd party.

Having identified the issue, a new version of the OVAL Schema has been prepared (5.9) and will be released in draft form in the next few weeks. There will be a short (6-7 week release cycle), with the intent of keeping this release simple, and minimize changes to the schema.

During the call, no feedback was provided for this release, and it will be implemented as described. Along with the draft of the Schema, there will be a web page describing the details of the release (https://oval.mitre.org/language/version5.9/index.html).

Release 5.10

There will be another planned release sometime in either May or July in order to accommodate the Developer Days scheduled in June. This timing allows either last minute discussion ahead of the release, or discussion about the just-released version at developer days.

The group was asked if there was a preference with the timing of the release

[Kent Landfield] Will there be a Winter Developer Days?

[Jon Baker] June Developer Days is planned for the week of June 4th a winter event is also being planned.

[Kent Landfield] Without a Winter Developer Days, there would not be a lot of opportunity to provide feedback for 5.10 release.

[Dave Waltermire] There will be a Winter Developer Days event, hosted by NIST, in March.

[Kent Landfield] That will help with concern regarding feedback.

[Jon Baker] A 5.11 release could also happen this year depending on community feedback.