OVAL Board Call – OVALDI License (10/19/2012)

Attendees

Eric Walker – IBM Corporation
Kent Landfield – McAfee, Inc.
Chandrashekhar B – SecPod Technologies
Randy Taylor – ThreatGuard, Inc.
Chris Wood – Assuria Limited
Anthony Busciglio – Cisco Systems, Inc.
Omar Santos – Cisco Systems, Inc.
Blake Frantz – Center for Internet Security
Scott Armstrong – Symantec Corporation
Steve Grubb – Red Hat, Inc.
Rob Hollis – ThreatGuard, Inc.
Steven Piliero – Center for Internet Security
Noah Salzman – IBM Corporation
Amaresh Shirsat – Symantec Corporation
Timothy Keanini – nCircle Network Security, Inc.
Dave Waltermire – National Institute of Standards and Technology (NIST)
Adam Montville – Tripwire, Inc.

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

Meeting Summary

Welcome and Historical Context

Jon Baker welcomed the group to the call regarding the status of the license for the OVAL Interpreter (also known as OVALDI), a reference implementation for the OVAL Language. Jon began by reviewing the history of the Interpreter's license, along with historical context around the related decisions. The following details were provided:

- Previous to the 4.0 OVAL Language release, the Interpreter was licensed using a GPL-style license.
- Prior to the finalization of the 4.0 Language release, there was an email thread on the OVAL Board list that discussed the state of the license, citing an RSA meeting as the starting point for a conversation to consider changing this license.
    - The discussion presented both pros and cons to a change.
    - Those in the 'pro' camp cited the GPL license as limiting the adoption of the OVAL Language because fear of contamination limited its use as a reference or within a product.
    - Those that were against a change voiced concerns that by using a less restrictive, open license, folks would be able to simply repackage the Reference Implementation within their own product and re-sell it.

- Out of a follow up Board Call, it was decided that a change of the license was justified and for the 4.0 release of the OVAL Language, the license was changed to BSD-style license and has remained under that license since then.

Following that introduction, Jon asked if the folks that were part of the community then remembered the discussion around the license in the same way.

- It was pointed out that in addition to the context given, which was correct, it was also stated that in order to guard against the re-packaging of the software concern, the OVAL Interpreter was to be clearly marked as a Reference Implementation and to be coded in a way that was not necessarily optimal.
    - Jon agreed with this point and added that the code has generally been developed in harmony with that description although there have been exceptions in some cases to make things work.
- It was also pointed out that there were 3 major uses of the Interpreter:
    - As a reference for the community to aid in OVAL Language implementation
    - As a way to exercise the OVAL Language ahead of releases to ensure quality and correctness of the OVAL Language
    - (Later on in its lifecycle) As a tool for NIST to use for the Validation Program

Current State

Shortly following the welcome, a discussion around the current state of the OVAL Interpreter and its license followed. The following were the relevant points made:

- The BSD license has some constraints on it. Any use of BSD-licensed software requires attribution and it is the responsibility of the license holder to follow up on these requirements.
    - It was conceded that MITRE could do more here to confirm the licenses requirements and MITRE will look into better understanding this obligation.
- It was suggested that MITRE could reduce or limit the functionality of the OVALDI.
    - One Board member replied that crippling a piece of open source software is generally not done and is a bad practice.
    - A related follow on point was made agreeing that typical open source software projects won't intentionally cripple the software.
    - It was widely agreed that MITRE needs to continue to focus OVALDI development around providing a simple command line utility and not address enterprise capabilities. That is, it may not require a license change, but rather, an increased awareness of the intended use and development goals of OVALDI.
- A general question about the ability of an FFRDC to do open source software development was raised. There was a concern that MITRE, which operates several FFRDCs, may be competing with industry by providing the OVALDI as open source software. It was asked that MITRE verify that this sort of open source development by an FFRDC is allowed.
    - A response reminded the group that the government funds many open source projects.
    - MITRE will talk to its corporate legal team to verify that this work is acceptable.

- One Board member suggested that one does not need a reference implementation to implement the OVAL Language because the specification(s) have become much more complete.
    - Others countered that it is still an important resource.
- It was pointed out that we should be most focused on the customer here and attempt to increase wherever possible, the value to the end user, and if tool vendors feel competition from the reference implementation, then it may be an indication that they must increase the value that their tool offers.
    - A response here was that it is difficult to compete with free, while others suggested that there still are a number of things that vendors can offer above the Reference Implementation.
    - Another response pointed out the people easily entering the market is a good thing.
- The challenges of changing an open source software license were also discussed.
    - One Board member mentioned that in order to change the license for a piece of software, one must either get the approval from all those that have contributed to the software, or to fork the software, neither of which are simple or desirable.
    - It was pointed out that all code contributions to the OVALDI have been fully transferred to MITRE and therefore we may not need to contact all previous code contributors. However, this would need to be verified.
- It was brought up that OpenSSL has had to go through a similar issue, when dealing with products like RSA's B-Safe.
    - Others argued that the OpenSSL situation was not analogous for the following reasons:
        - OpenSSL was not certified, which made it less desirable and potentially impossible to use.
        - The authors of OpenSSL were not an FFRDC and therefore the development was not paid for by tax dollars.
    - This lead to the general agreement that it must be clearly noted that the OVALDI will never be validated through any formal validation program by MITRE.
- Several vendors mentioned that the OVALDI is not an issue for them, though they generally understood the argument against the current licensing.
- Jon reiterated the use cases that are served by the Reference Implementation and pointed out one additional use case on top of those previously mentioned:
    - Reference for other OVAL vendors to use as a way to understand how the language is to operate
    - Ability to use implementation of the language to ensure OVAL Language quality and correctness (PowerShell implementation was cited as an example here)
    - Support of the Validation Program
    - Developing and testing OVAL content
- A question was asked about confirming the attribution portion of the BSD license. Specifically, since BSD requires that attribution be given to the authors of the code, is anyone confirming that those using the OVAL Interpreter are correctly following this requirement?
    - MITRE will look into how to fulfill this obligation if necessary.

- Also it was highlighted that while the Reference Implementation is useful for content authors to test their content, source code access is not required for this activity.
    - The reverse argument was also given, suggesting that in some cases the source code is very important to content authors when the content is not interpreted the way they intended.
- It was suggested that the MITRE team should poll the community to better determine how the Reference Implementation is being used and by whom.
    - It was agreed that the results of this survey should be shared.
    - MITRE will poll the OVAL Adaptors, OVAL Board, OVAL Developer List, and talk to NIST about polling the SCAP Validated vendors.

Actions

As actions from this phone call, the following will be done:

- MITRE to poll the community (The Adoption program participants, the OVAL Board and/or Developer lists, and potentially those in the NIST Validation Program) in order to determine who is making use of the Reference Implementation and how.
- MITRE to follow up with what (if any) bounds the Corporation has on what it can contribute to open source software.
- MITRE to follow up, once the results of the survey are gathered, with another call with the Board to discuss results of the data gathering and to decide on next steps.
- MITRE to make some updates to the relevant web sites to make it more prominently stated that the Reference Implementation is for reference only and is not a certified scanner. This will include prominent suggestions to look to the list of OVAL Adopters and clearly articulate the intended purpose of the OVALDI.