OVAL Board Meeting (1/14/2013)

Attendees

Anthony Busciglio - Cisco Systems Inc.
Dave Waltermire - NIST
Eric Walker - IBM Corp.
Kent Landfield - McAfee Inc.
Aharon Chernin - DTCC
Omar Santos - Cisco Systems Inc.
Steve Grubb – Red Hat Inc.
Randy Taylor – ThreatGuard, Inc.
Chris Wood – Assuria Limited
Blake Frantz – Center for Internet Security
Carl Banzhof – Rockport Systems
Jean Reese – Cisco Systems Inc.

Jon Baker - MITRE
Matt Hansbury - MITRE
Dan Haynes - MITRE
David Rothenberg - MITRE

Meeting Summary

Welcome

After introductions the group was welcomed to the 2013 1st quarter OVAL Board Meeting. One new Board member was introduced to the group:

William Munyan – Center for Internet Security

Additionally, one Board update was given. Steven Piliero has moved to Unified Compliance.

Status Update

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

OVAL Adoption

Declarations

- Pivotal Security LLC for their Security Scanning SDK
- Institute for Information Industry for their Crystal Security Keeper product

OVAL Language

A brief update of the OVAL Language was given. The OVAL project celebrated its 10 year anniversary in December of 2012. This is a significant milestone for the project and indicates a longevity and maturity that has been highly dependent on the community, and in no small part, the hard work of the OVAL Board members. A MITRE press release is going to be published to commemorate the anniversary.

The OVAL team is now focused on the 5.11 release of OVAL. Several research projects have been undertaken and are going to make their way to the OVAL Language Sandbox for vetting over the next few months. Additionally, the team announced that the OVAL Language Schema files would be hosted on GitHub moving forward, in order to provide more transparency and clarity into changes made from version to version.

Additionally, updates on two major areas of focus were given. The first update involved the Mobile Devices space. The OVAL team has been researching the Android platform and has created a proof of concept application that takes an OVAL Definition and generates a System Characteristics file on an Android device. This output can then be evaluated on a different machine using a Definition Evaluator tool. The source code for the proof-of-concept will be made available in the OVAL Language Sandbox once it has gone through the review process. Based on the lessons learned, the team will additionally be providing feedback on the experimental Android schemas developed by the SecPod Technologies Team. These changes will be made in the OVAL Language Sandbox.

Secondly, the OVAL team has also developed a prototype for the sql57_test in the OVAL Interpreter for Windows and Linux and it is currently available in an OVAL Interpreter branch. As of right now, it has been tested on MySQL, but, there are plans to test it on additional databases. Sample content, based on the CIS Benchmark for MySQL, is also available in the OVAL Language Sandbox. This prototype and sample content will provide the community with a working implementation to experiment with and will help the community to better understand how the Schema or documentation might need to be updated to better reflect practical applications.

Lastly, the Cisco team has submitted two new component schemas for their Cisco IOS-XE and Cisco ASA platforms. These schemas are available in the OVAL Language Sandbox.

OVAL Interpreter

The OVAL team published version 5.10.1.4 of the Interpreter on December 21st. Support was added for scheduling_class entity in the UNIX process tests and numerous bugs reported by the community were fixed.

OVAL Repository

The OVAL Repository's definition count at the time of the call was 14,278. ALTX-SOFT, G2 Inc., and SecPod Technologies received the Top Contributor Awards for the 4th quarter of 2012 for their submissions to the OVAL Repository.

OVAL Interpreter Discussion Follow Up

Following the 2012 Q4 OVAL Board call, there was an additional phone call held to discuss the OVAL Interpreter following some concerns about the licensing model and some potential issues it could cause with respect to competitiveness. The OVAL team gave an update on their action items from that call.

Website Updates

The team made several website updates to more effectively describe the purpose of the OVAL Interpreter. The following updates were made:

- A more clear description was given on the OVAL Interpreter page to better articulate the purpose of the Interpreter and to highlight that it is not intended for commercial use.
- Use Cases for the Interpreter were added to make it clearer that it primarily is developed as a reference implementation and to test the Language.
- Additional links and wording was added to more directly highlight the OVAL Adoption program for those looking for commercial vendors and tools that support OVAL.

All of these updates can be seen on the OVAL Interpreter page on the OVAL web site: https://oval.mitre.org/language/interpreter.html.

Legal Information

The OVAL team has begun reviewing with its legal team exactly what policies and procedures are required for MITRE-coded Open Source projects. This information gathering is still in process and an update will be provided when available.

Survey Results

The OVAL team then gave a detailed review of the responses to a survey sent out in response to the concerns regarding the OVAL Interpreter license. Overall, there were 22 total responses, 6 from organizations represented on the OVAL Board, and 14 organizations participating in the OVAL Adoption program.

The team reviewed each of the questions and gave an overview of the answers provided. The results of the survey will be sent out by the team in the near future.

The overall conclusions supported by the survey results were the following:

- The OVAL Interpreter is used widely in the community for content testing, product testing, and as a reference. It is also used in commercial products in some cases.
- The majority of the respondents seem to be happy with the OVAL Interpreter as a reference implementation and several would like to see more done to improve quality of language and interoperability of tools.
- Respondents who are directly using the OVAL Interpreter or its source code are making efforts to follow license and copyright requirements.
- Based on these results, there does not appear to be a compelling reason to change the OVAL Interpreter license.

General Discussion on OVAL Interpreter

Following the results of the survey, there was a bit of general discussion from the Board on the topic. This captures the main points made:

- It was asked how the team prioritizes its Language work. There is no formal process, but, the team manages the work by determining critical areas through community discussion and addressing critical defects in the code base. The OVAL Community is strongly encouraged to provide specific areas of interest to help the team to best prioritize its work.
- Write access for the OVAL project's source control was discussed. The questions revolved around a potential process for granting write access to non-MITRE developers/organizations. This also touched on the maturity of the project and the potential for moving to a formal international standards body. The team pointed out that contributions to the project are always welcomed and encouraged, but added, that it can take significant effort from them to review code contributions, provide feedback, and integrate them into the codebase. It was suggested also that up until this point there really hasn't been enough consistent contributors to make such a policy relevant. A reply to this position was that with or without the acute need, having such a process in place would contribute to the maturity and transparency of the project.
- The idea of creating a sub-group was floated to address the general maturity of the project, with respect to the potential transfer to a formal international standards body. Several Board members volunteered for such a group.

Solaris Patch Testing

It was brought up over the mailing lists that there was some difficulty with assessing the newer versions of Solaris. The current capabilities of the Language do not allow the proper testing of the platform, leaving vendors to either not test the platform or to write custom checks. A general conversation about the topic occurred:

- The question was asked if this involved the ksplice project, which allows updates directly to the binaries, thus avoiding reboot. This was not the intent of the question.
- It was pointed out that this work would be a very good fit for the OVAL Sandbox as a way to get a notional Schema out to vendors for feedback and potential implementation.
    - Vendors showed reluctance to this, because their company policy would not allow support of such an out-of-release version of the Schema.
- Others pointed out that some conversation with Oracle had occurred and they might be able to help here. Blake Frantz offered to help with a contact on the Oracle team.
- An informal poll was taken to see how many vendors are supporting Solaris, with 4 or so claiming to support or having plans to support, Solaris. (Note: this was actually 4 out of the 6 vendors on the call)
- The appropriate way to move this forward, it was suggested, was to model the tests, provide draft Schema, and then work with the community on vetting it and moving it into the Language.

Additional Items

Following the end of the formal agenda, the floor was opened. One item was raised:

- Blake Frantz noted that CIS was in the process of creating benchmarks for Kerberos and in doing so was finding the need for a specific test to evaluate .ini files. He asked the group if others saw value in such a thing.

  - It was agreed that in some cases file formats proved to be challenging to work with and in those cases, a custom test would be appropriate.
  - It was also pointed out that since one of the key issues with OVAL is lack of content in some places, ease of content authoring was important.
  - Blake concluded by offering that the CIS team would consider the creation of Schema updates and documentation for such a test and will work with the community to help to implement this in the OVAL Sandbox.
  - A tracker item was opened to cover this feature: https://github.com/OVALProject/Sandbox/issues/19

Action Items

- MITRE to resend the details of the OVAL website update clarifying the OVAL Interpreter purpose.
- MITRE to send out the Survey Results, initially to the OVAL Board, and then the broader community.
- MITRE to research what steps can be taken to confirm that the organizations that have attested to following the OVAL Interpreter licensing requirements, have done so correctly.
- MITRE to add a tracker for the Solaris patch testing work: https://github.com/OVALProject/Sandbox/issues/62