OVAL Board Meeting (10/18/2010)

Attendees

Nick Connor – 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
Scott Armstrong – Symantec Corporation
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.

Jonathan Baker – MITRE
Matt Hansbury – MITRE
Danny Haynes – MITRE
Mike Lah – MITRE
Charles Schmidt – MITRE
Margie Zuk – MITRE

Meeting Summary

Welcome

The group was welcomed to the 2010 4th quarter OVAL Board Meeting. A new member, Aharon Chernin from DTCC, was welcomed to the OVAL Board.

Status Report

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

OVAL Language

The major milestone for the OVAL Language was that Version 5.8 was released on September 15th, 2010. This release signified a lot of hard work from the OVAL Community including the introduction of several new tests and improved documentation in the schemas. The UNIX and Linux component schemas grew in large part due to Steve Grubb and we would like to thank him for his support in that effort. Additionally, this release featured the refactoring of many Schematron rules into XML schema by Jasen Jacobsen. This refactoring significantly reduced the amount of time needed to perform Schematron validation on an OVAL Document.

OVAL Repository

On September 16th, 2010, the OVAL Repository surpassed the 10,000 OVAL Definitions marking a significant milestone in its history. The top contributors to the OVAL Repository this quarter were DTCC, SCAP.com, LLC, SecPod Technologies, and Symantec, Inc.

OVAL Interpreter

Version 5.8.2 of the OVAL Interpreter was released on October 15th, 2010. This release primarily focused on bug fixes in the OVAL Interpreter, the most notable of which was to update the existing probes to align with the datatypes that were corrected in Version 5.8 of the OVAL Language. Prior to this bug fix, the OVAL Interpreter was outputting invalid schema.

OVAL Adoption

Currently, we only have a few questionnaires. This is because we need to improve and mature the questionnaire prior to asking additional organizations to fill it out as some of the questions are ambiguous. If you are on the OVAL Board, and you have a product or service that is using OVAL that is not in the OVAL Adoption Program, we would appreciate it if you would take the time to fill out an OVAL Adoption Declaration. We would really like to see how the OVAL Community is using OVAL in their products and services as well as get their feedback. In the upcoming weeks, we will be sending out additional questions regarding the questionnaire in order to improve it so that we can start moving organizations into the second phase of the OVAL Adoption Program.

IT Security Automation Conference (ITSAC) Recap

This year's IT Security Automation Conference was well attended and OVAL was also well represented as it had three different sessions. The first session was an OVAL Tutorial given by Matt Hansbury which focused on what OVAL is and how it works. The second session was an OVAL Status Update given by Jon Baker which focused on the releases of the OVAL Language since Version 5.0 as well as the key changes made in each of them. Finally, the last session was the OVAL Workshop, also led by Jon Baker, which focused on getting the OVAL Community to start thinking about what we should do next with the OVAL Language and more specifically:

- How do we make OVAL more maintainable?
- How do we make OVAL easier to implement?
- How do we make OVAL more scalable to allow for the support of new platforms?

The slides from the OVAL sessions as well as the minutes for the OVAL Workshop at the IT Security Automation Conference can be found at the following links.

OVAL Session Slides

OVAL Tutorial - https://oval.mitre.org/oval/about/2010_ITSAC-OVAL_Tutorial.pdf

OVAL Status Update - https://oval.mitre.org/oval/about/2010_ITSAC-OVAL_Status.pdf

OVAL Workshop - https://oval.mitre.org/oval/about/2010_ITSAC-OVAL_Workshop.pdf

OVAL Workshop Minutes

https://oval.mitre.org/oval/about/OVAL_ITSAC_Workshop_2010-09-29_Minutes.pdf

As a result of the workshop at the IT Security Automation Conference, we will be following up with further discussion over the oval-developer-list in the next few weeks.

IETF SCAP BoF Discussion

This topic was raised by Kent Landfield in order to explain to the OVAL Board what the IETF SCAP BoF session will be about and explain the reasons for having the session and the goals for the session. It also provided an opportunity to address any questions or concerns that the members of the OVAL Board might have.

[Kent Landfield] The purpose of the IETF SCAP BoF in Beijing China is to introduce SCAP to the IETF as well as learn about the IETF. The IETF fits well with SCAP and is aligned with the approach we have taken in developing SCAP as a community. SCAP while received well in the U.S., has not yet been widely adopted internationally. SCAP is ready to be introduced to an international audience. We are going to be very selective with what is proposed to the IETF in that it needs to be very stable and well adopted. We are not suggesting everything at this time. Given that XCCDF is fairly stable and well understood, it is likely a good first candidate for the IETF.

[Rob Hollis] What would it mean to bring only part of SCAP to the IETF? Won't it be incomplete?

[Kent Landfield] We are not taking anything to the IETF yet. We are introducing the idea as it takes effort to get standards approved. We need to get the entire suite there at some point.

[Jon Baker] It is important to remember that as we are today, no single organization controls SCAP and all the protocols it references. For example, NIST controls SCAP as defined in 800-126 while DHS has been funding OVAL and NSA has been funding CPE and CCE. Taking one or more of the SCAP protocols to an international standards body would simply introduce another controlling organization into the SCAP world.

[Kent Landfield] This is also a defensive move for the community. If SCAP is not introduced to an international standards body, similar or competing efforts will be created by others. This will only lead to duplication of our efforts and implementation challenges for vendors that are required to support SCAP and other potentially competing efforts.

[Melissa Albanese] What standard is most at risk of this competition XCCDF, CVE, CCE, etc.?

[Kent Landfield] CVE is one example. We have had to do this reactively.

[Jon Baker] This already happened with CVE, and is largely the reason for CVE appearing in ITU-T x.cybex.

[Dave Waltermire] We hear that from vendors.

Is OVAL Ready to be an International Standard?

Given the interest in IETF and the notion of introducing SCAP to an international audience, we need to consider where OVAL is today. This portion of the call focused on understanding the OVAL Board's perspective on OVAL's readiness to become an international standard. The key questions for this discussion were:

- Should we prepare OVAL for some international standards body?
- What are the current deficiencies?
- What would it take to prepare OVAL?

[Rob Hollis] What does it mean to be an international standard? Does the standard need to be static, as OVAL is continually evolving?

[Kent Landfield] Many protocols, such as email, have evolved over time and over different RFCs. It doesn't mean that the standard needs to stagnate.

[Dave Waltermire] Some only standardize the core. Examples of this are MIBs and NETCONF. Look at only standardizing the core schemas of OVAL, but, not the component schemas allowing the core schemas to evolve more slowly whereas the component schemas could evolve more rapidly.

[Eric Walker] In response to the question of whether OVAL is ready, OVAL is not ready. It appears as though OVAL was originally inspired on the model of HTML or perhaps some other precursor. [To clarify -- something along the lines of the Java approach to XML configuration files, e.g., a Tomcat configuration file. --EW] Over the last 10 or so years or so a number of best practices have emerged [that are counter to the spirit of complex configuration files and the whole approach of enterprise software development more generally -- e.g., convention over configuration; piecemeal, incremental refactoring of something that is basic but does the job; agile development and avoiding complex designs up-front if possible; RESTful services, etc.]. [In light of these developments, one gets the sense that] OVAL has become unwieldy. To be ready we need to be prepared to rework OVAL from the ground up. I wouldn't mind talking about this in further detail with you.

[Jon Baker] Let's set something up offline or with a follow up board call.

[Kent Landfield] OVAL isn't ready because we need a specification. We have been working from schemas. We cannot just throw them in a document and call it a standard. Maybe with a thorough specification document your concerns will be addressed? In short, I say no. OVAL is not ready for a different reason. It is not because we don't have a good capability, but rather we don't have a spec.

[Aharon Chernin] We need a driver for vendors other than the federal space to drive the standards forward. I would like to see SCAP go to the IETF from a customer perspective.

[Melissa Albanese] Could you still make the types of changes that were discussed at the OVAL Workshop held at the ITSAC when it is an international standard?

[Jon Baker] Good question. We have been thinking about that and many of the topics would need to be thought through working together with the community and would likely require another revision of the language before it could even make it as an international standard. The idea has been to make some smaller changes to OVAL to position it such that OVAL could be taken to an international standards body.

[Kent Landfield] The more basic question, does it make sense to make OVAL an international standard?

[Scott Armstrong] Yes. With all of these vendors and repositories popping up, we would need to do more work, but, I think it should be an international standard.

[Steve Piliero] We work with a lot of international organizations and we find that many of them are reluctant to use the SCAP standards because they are U.S. Government standards and are not from some international standards body.

[Luiz Nunez] I want to thank Kent for heading up this discussion. It's a good effort.

[Melissa Albanese] It's a good idea to move with making OVAL an international standard. We try to push for international standards and it is where we would like to see things go.

[Jon Baker] We would like to continue this discussion. Now, we have to see where we go next. I think Version 5.8 puts us in a good position though. We are beginning to work on a specification and when we have more concrete thoughts on the specification we will share them with community through drafts. We would also like to work with the community to determine what to do for Version 5.9. And yes, as Melissa said, we talked about specific issues at ITSAC and they are things we need to start talking about over the community mailing list.

OVAL Board Membership Discussion

We regularly receive requests from members of the OVAL Community to become members of the OVAL Board. Traditionally, it has been the responsibility of MITRE and the OVAL Team to make the decision as to whether or not a prospective OVAL Board member is actually added. Given that it has been a MITRE decision, we would like to provide insight into how we currently process these requests, present two different options as to how it could be changed, and get your feedback as to whether or not the current process makes sense or if it should be changed. The key questions for this discussion were:

- How do we identify new OVAL Board members?
- How do we vet/approve new OVAL Board members?

[Jon Baker] Over the last several years, we tried to ensure that the OVAL Board is well mixed with active members to advance the effort and not just to serve as a badge for marketing. We want to make sure that numerous perspectives are represented: the end-user perspective, the vendor implementer perspective, and so on. We try to keep the OVAL Board around 30 members because it may become too unwieldy if we go beyond that. We have been considering different ways to determine OVAL Board membership. Should we make it so prospective OVAL Board members must be nominated by the current board members? Should we have an approval process for vetting new OVAL Board members

where the OVAL Board would approve the candidate? The upside to reconsidering how we do this is that it gives the OVAL Board more control of who is on the OVAL Board and what the OVAL Board is. Should we leave it as a MITRE and OVAL Team decision?

[Morey Haber] Any company that supports OVAL and is using OVAL should have a spot on the OVAL Board as they are supporting it by developing a product and should have the ability to see what is going on in the future.

[Scott Armstrong] They should have to be active and not just listeners.

[Kent Landfield] I agree with Scott. You should have a stake in OVAL. If you are a vendor, and you are supporting OVAL, you should have a spot, or at least a chance to have a spot, on the OVAL Board. Those who don't have a stake don't have a spot.

[Dave Waltermire] What are we trying to accomplish with the OVAL Board?

[Rob Hollis] I think of the OVAL Board as steering committee for the OVAL Community and should be active.

[Melissa Albanese] Are there a lot of people asking to be on the OVAL Board?

[Jon Baker] New OVAL Board membership requests tend to come in waves. We seem to average about one new request per month. We also had a lot of requests after the SCAP Validated products came out.

[Melissa Albanese] In the past we have weeded out people, how do you think that has worked?

[Jon Baker] Over the multiple quarterly OVAL Board calls, I would say we currently get fairly good attendance. We don't really have many board members that routinely do not participate.

[Melissa Albanese] I would say that we should be more inclusive and then if people are not participating, we should remove them.

[Carl Banzhof] This may be an opportunity to introduce a dual board: one to deal with technical side and another, advisory board, for the business side to get OVAL adoption out there and beyond the federal government.

[Jon Baker] On the OVAL website, there are a couple of short paragraphs that describe the role of the OVAL Board (https://oval.mitre.org/community/board/). The OVAL Board is described as follows:

"The OVAL Board is an advisory body, which provides valuable input on OVAL to the Moderator (currently MITRE). While it is important to have organizational support for OVAL, it is the individuals who sit on the OVAL Board and their input and activity that truly make a difference. The Board's primary responsibilities are to work with the Moderator and the Community to define OVAL, to provide input into OVAL's strategic direction, and to advocate OVAL in the Community.

Each OVAL Board member is expected to meet the following requirements:

- *attend the quarterly board meetings (telephone calls)*
- *provide input into OVAL's strategic direction*

- *actively follow and participate in both the discussion and developer email lists*
- *provide expert advice about OVAL to the Community*
- *look for opportunities to advocate OVAL in the Community*

In addition to the above requirements, an OVAL Board member is expected to look for opportunities to include OVAL in his or her organization's products.

In an effort to guard against organizational bias, a single organization may be represented by a maximum of two individuals with the expectation that one individual would be focused on strategic direction and the other individual would be focused more on technical decisions.

If you are interested in becoming an OVAL Board member email oval@mitre.org. Potential members should be participants in the Community before looking to join the OVAL Board. The OVAL Moderator has the final say regarding membership."

[Dave Waltermire] If OVAL has specification at IETF, what will the OVAL Board's role be and what will MITRE's role be?

[Kent Landfield] The discussion of what makes the most sense there are longer run discussions and are probably not a discussion that we need to have right away, but, it may be good to have a time table to get them in there.

[Dave Waltermire] We may be interested in the ratio of the OVAL Board. We have government, vendors, end-users, and so on. Maybe we want more international representatives?

[Jon Baker] Yeah, that is a good idea.

[Steve Piliero] With simple goals of guidance and roles of standards, we will have a better idea of who we need to have on the OVAL Board.

Action Items

- Hold a follow up teleconference to discuss in detail the feedback and concerns that BigFix expressed.
- Work with the OVAL Community to improve the OVAL Adoption questionnaire.
- Begin discussion on the development of an OVAL Language specification.
- Follow up with the OVAL Workshop discussion held at ITSAC over the oval-developer-list.