OVAL Board Minutes
2008-07-14

Attendees

Jonathan Baker – MITRE
Andrew Buttner – MITRE
Bryan Worrell – MITRE
Rob Hollis – ThreatGuard Inc.
Melissa Albanese – DoD
Jay Graver – nCircle Network Security, Inc.
Nick Connor – Assuria Limited
William McVey – Cisco Systems
Dave Waltermire – Booz Allen Hamilton
Pai Peng – Hewlett Packard
Kent Landfield – McAfee
Carl Banzhof – McAfee
Jim Hensen – BigFix Inc.

Agenda

- welcome
- status update
    - ongoing contributions for windows, hp, solaris
    - reference implementation update
    - presence at black hat
    - compatibility
    - schema development
        - 5.5 is on the roadmap
- minor release ideology
    - should we fix bugs or hold true to not invalidating
    - should we change policy now or wait until 6.0
- 2008 Developer Day follow-up
    - thanks again for participation
    - notes have been circulated
    - starting work on action items
        - issue tracking
        - sandbox
- version 6.0 plan
    - continuing open conversations on list
    - will start working on a draft toward the end of July
    - still on track for a 1st draft by the Fall
- remediation
    - does a remediation schema still fit into the v6 plan?
- OVAL Compatibility plan
    - update on talks with NIST
    - comments from Board
- questions / concerns

Meeting Summary

Welcome
Introductions regarding who was on the call and an overview of the agenda were made. It was mentioned that the previous board meeting had been missed.

Status Update
Overall, OVAL continues to grow and gain acceptance within the industry. There are now 5 different platforms that receive regular updates from various members of the community. These platforms are Windows, HP-UX, AIX, Solaris, and Novell. This is in addition to Red Hat and Debian that produce their own OVAL content.

The move to SourceForge has been a huge success for the reference implementation. Recent effort has been on fixing some of the bugs that the community has found and reported.

A quick mention was made regarding OVAL's presence at the upcoming Black Hat conference. OVAL will be part of MITRE's Making Security Measurable booth. If anyone is going to be at the conference they are encouraged to stop by.

OVAL Compatibility and schema development were deferred until later in the call. The only point mentioned at this time was that Version 5.5 will happen and that although no dates have been given, a late summer timeframe would make sense.

Minor Release Ideology
Some recent issues with the schema have been discovered and some in the community have asked that a change to the schema be made immediately. The question was posed to the board, specifically whether we should stand by the documented approach of not invalidating existing content, or whether we should make exceptions for certain issues. Some support for both sides was given, the final word was to not invalidate. Creating new tests and deprecating existing ones should not be painful.

This sparked the following discussion:

Rob Hollis:	We should set up a policy for bug fixes and updates that lies outside of the standard release policy.
Andrew Buttner:	By defining exceptions to the rule, we can establish a policy for updates outside of the standard release cycle.
Rob Hollis:	One such example could be spelling errors.
Melissa Albanese:	As invalidating existing content is a concern, I purpose that when fixing an issue such as a misspelling, we should continue to create a duplicate item that is spelled correctly and deprecate the misspelled item.
William McVey:	Maybe we should consider a stylesheet which extracts deprecated items upon processing against a content submission. This would allow the user to see that they are using a deprecated feature. A more advanced stylesheet could automatically update the deprecated feature.
Andrew Buttner:	That is something to consider.
Dave Waltermire:	Schematron already has some of this built into it with multiple phase functionality that would enable different levels of validation depending on what phase was specified.

OVAL Developer Days
OVAL Developer Days was held this past spring and by all accounts it was another great success. 30 plus community members were in attendance and many of the issues facing OVAL were discussed. Detailed notes have been circulated and the OVAL Team in now in the process of working on the action items that came out of the 2 day session. In the coming weeks there should be a number of different threads started on the developer list as we address each issue and work on the development of version 6.0.

Version 6.0

OVAL version 6.0 is on schedule for a first draft sometime this coming fall. The process of developing and pushing this out will most likely follow the one set by version 5.0.

Kent Landfield: I think we should post an outline of what version 6.0 is going to address.

Andrew Buttner: Great point, we will take this on as an action item. Related to this, we are looking to make our internal tracking application visible to others via the OVAL website.

Remediation

The next topic of discussion for this meeting was in regards to a remediation schema for OVAL. This is a topic that has been dreamed about for a while but has just recently started to gain some serious momentum. The community first discussed it at OVAL Developer Days and since there has been some further discussion on the repository working group list.

Jonathan Baker: I would like to encourage you all to follow the conversation on the remediation list regardless of whether or not you feel you have anything to contribute to the discussion.

Jonathan Baker: Remediation is proposed as a new (4^{th}) component to the OVAL Language, similar to the Definitions schema, the System Characteristics schema, and the Results Schema.

Kent Landfield: Remediation was something that was supposed to be utilized by OVAL and not shoehorned into the language. By putting this inside of OVAL, you limit how much can be done on the remediation side. For example, remediation may need a different regex language than what is found in the rest of OVAL.

Jonathan Baker: Definition content shouldn't be interwoven with the Remediation schema. Someone who is only concerned with the structure of the Definitions schema shouldn't have to worry about the Remediation schema or Remediation constructs being embedded within the Definitions schema. By developing this as a complete separate schema similar to how the SC and Result schema are we will hopefully have the flexibility to do what we need to do.

Kent Landfield: Simply put, I want architectural consistency.

Jonathan Baker: What we are hoping to do is discuss remediation, understand what it needs to support, and what constructs might be needed. Then determine if this can fit as the proposed 4^{th} schema. If it doesn't fit within OVAL then we can work to set this up as a separate project. But for now let's work on better understanding the problem.

OVAL Compatibility Update

MITRE and NIST continue to make progress on addressing the proposed transition of the OVAL Compatibility program over to NIST. We are currently putting the finishing touches on a document that will outline the roles of each organization and when finished, this document will be given to the OVAL Board to read and discuss. A high level overview of the proposed program was given. The following points were made after the overview:

Jay Graver: The NIST website will have a list of validated applications.

Jonathan Baker: I am not sure how much the validation is going to cost, but I would assume that the fee should reflect the level of complexity around the validation.

Melissa Albanese: Can someone pass validation if they do not support certain types of tests, such as WMI? Have

Jonathan Baker: We might need to consider different levels of certification.

Dave Waltermire:	Certification would be on a per-platform basis, so if a person is attempting to achieve a Windows certification but lacks support for WMI tests, they will fail.
Jonathan Baker:	It should be about one month to six weeks before we start to see a transition to the NIST site.

Questions / Concerns

There were no additional questions or concerns.

Action Items

- Better define what is allowed in a major and minor update.
- Develop policy for how to handle certain change requests and outline what to expect from the process.
- Send a version 6.0 summary to the developer list.