OVAL Board Meeting (04/12/2010)

Attendees

Jonathan Baker – MITRE
Matt Hansbury – MITRE
Danny Haynes – MITRE
Mike Lah – MITRE
Bryan Worrell – MITRE

Chris Wood – Assuria Limited
James Hansen – BigFix, Inc.
Blake Frantz – Center for Internet Security (CIS)
Luis Nunez – CISCO
Melissa Albanese – DoD
Morey Haber – EEYE
Dennis Moreau – RSA
Scott Armstrong – Symantec Corporation
Timothy 'TK' Keanini – nCircle Network Security, Inc.
Dave Waltermire – NIST
Steve Grubb – Red Hat
Randal Taylor – ThreatGuard, Inc.

Meeting Summary

Welcome

The group was welcomed and thanked for attending the 2010 2nd quarter OVAL Board Meeting. The new members of the OVAL Board were welcomed and announced. The new members were:

- Luis Nunez of Cisco
- Michael Tan of Microsoft
- Steve Grubb of Red Hat

Status Update

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

OVAL Language

- Version 5.7 will be delayed by 4 weeks in order to address the following issues with n-tuple support:
    - Documentation of how the record datatype handles variables
    - There is no way to specify records in external and constant variables
    - There is no way to specify which field in a record should be retrieved when using an object_component

- It would be possible to push out the new release, but dealing with these issues will prevent a lot of confusion with the record datatype.
- We have started work on the highest impact changes for Version 5.8:
    - Cleaning up and refactoring the Schematron rules. Last count, ~3000 rules can be factored out and replaced with XML schema constraints instead. This will be easier for tools to support, and the burden of processing Schematron will be greatly decreased.
    - In alignment with the idea of minor releases, Version 5.8 will keep backwards compatibility with previous versions of the language.
- Questions?
    - How will the delay of Version 5.7 affect the release of Version 5.8?
        - Given the four week delay of Version 5.7, and the fact that Developer Days is in June, we propose pushing back the release of Version 5.8 by two weeks to allow time to incorporate feedback from Developer Days. However, a hard date has not been set.

OVAL Interpreter

- The OVAL Interpreter ports for Mac OSX and Solaris are available on the OVAL Interpreter SourceForge project site:
    - Mac OSX: http://ovaldi.svn.sourceforge.net/viewvc/ovaldi/branches/macos_port/
    - Solaris: http://ovaldi.svn.sourceforge.net/viewvc/ovaldi/branches/solaris_port/
- We currently do not have native binaries available. However, we will start back up with building native binaries and adding support to the ports after we finish getting the OVAL Interpreter ready for Version 5.7.

OVAL Repository

- The repository is approaching the 7000 definition mark; at the last board meeting in October it was 6000, so a lot of progress on that front. There is a good group of active contributors leading this effort.
- The "Top Contributors" this quarter were DTCC, Hewlett-Packard, and Symantec, Inc.
- Thanks to everyone for keeping the repository up to date with Microsoft advisories, and other current issues.

OVAL Adoption & OVAL Validation

- There are now 13 organizations and 20 products participating in the OVAL Adoption program. We would love for all products using OVAL to be included, and encourage you to apply.
- The OVAL Validation DTR (NIST IR-7669) has been posted. Please check it out and make comments. Once the comment period expires and the comments are addressed, the OVAL Validation program and the labs will be set up.

Version 5.7 Summary & Update

Version 5.7 brings with it a number of significant changes:

- Support for n-tuples

    - Support queries to system repositories that return multiple fields in one record. This is in response to OVAL Community feedback.
    - Added new tests (ind-def:sql57_test, ind-def:ldap57_test, win-def:wmi57_test, and win-def:activedirectory57_test) in order to leverage n-tuple support.
        - Also deprecated the old versions of these tests.
- Numerous Schematron rule refinements and performance focused improvements.
- Significant documentation improvements were made throughout the OVAL Language schemas.
    - Responses to questions on the oval-developer-list show up in the documentation.
- Removed the long deprecated ind-def:filemd5_test and apache-def:version_test and all their related objects, states, and items.
- New tests and component schemas added in Version 5.7
    - Added the win-def:dnscache_test and unix-def:dnscache_test to support checking the dns cache on a local host.

Version 5.7 RC4 will be posted by the middle of this week, with an official release date of May 12th 2010.

Release Timeline for Version 5.8

Currently, the Version 5.8 schedule is:

- DRAFT - 5 May 2010
- RELEASE CANDIDATE - 7 July 2010
- OFFICIAL - 4 August 2010

We are also considering moving the timeline for Version 5.8 back a couple of weeks to accommodate Developer Days.

OVAL Developer Days Planning

Developer Days has become our annual opportunity for everyone involved in developing OVAL Products, policy makers, and content creators to get together and discuss the future of OVAL. N-tuple support and the recent updates to the Schematron rules were a result of discussions at last year's Developer Days. This event really has a big impact on shaping the language. We continue to have active discussions on the mailing list, but face-to-face interaction is really important.

This year's Developer Days is scheduled for the middle of June (June 14-16), and we have a half day scheduled for OVAL. We would like to present interesting capabilities that we have in mind, like support for XML as a value. OVAL currently supports string, int, and boolean values, but we want to discuss different ways to implement XML values.

Thanks to Steve Grubb from Red Hat for lots of feedback on the Linux schema as he has been working on OpenSCAP and security guidance development for Red Hat systems.

The OVAL session will first highlight some of the significant updates since the last developer days and then shift focus to considering future directions for OVAL. We will discuss minor capabilities appropriate for version 5.8 and also larger changes suitable for the next major revision.

Questions / Other Issues

Versioning of Content

Dave Waltermire: Related to Version 5.7 release process and building support to reference OVAL Definitions out of the NVD. SCAP lags behind OVAL releases by several revisions. SCAP 1.0 uses OVAL 5.3 and OVAL 5.4. SCAP 1.1 uses OVAL 5.6. One concern is the version of the content in the OVAL Repository. If SCAP is at Version 5.6, and the repository content is upgraded to Version 5.7, there is a risk that tools supporting SCAP will not be able to process some of the OVAL Repository's content. We would like to develop a best practice that would express content in the minimum version required. We would prefer that OVAL not upgrade all of the content because it falsely represents that the content has been upgraded to newer tests when it may not need to be. Are there any thoughts on this?

Jon Baker: From our perspective, trying to implement a least-version principle in the repository would become a resource issue. It suggests a re-architecting our infrastructure, as we would be serving up content in multiple versions. It wouldn't be terribly hard to do, but it would require us to be capable of searching for definitions in multiple versions. This is a challenge for tool vendors to think about.

If the OVAL Repository supports multiple versions, this could pose a challenge to content creators potentially having to write multiple versions of definitions. We need to reduce the burden on content authors and should stay away from requiring them to know which minimum version of the OVAL Language each and every definition relies upon.

An additional issue is what to do with submissions. Is there a way to take submissions and somehow "cast" them down to the last version in which it can be expressed? When you serve up the definitions, would you have to "cast up" for users that want only the latest version of OVAL?

Dave Waltermire: This becomes more complex when we talk about spanning major versions of OVAL. We are trying to minimize the effort required to create content.

Jon Baker: This seems like a good topic of discussion for Developer Days; Dave Waltermire would you like to collaborate on this? Is there anything else that we would like to discuss regarding OVAL at Developer Days?

Steve Grubb: We could talk about what will be required with the DoD baselines from DISA, what goes in reports, and why these things are needed as well as hints on possible implementation.

Jon Baker: Some of the things that you have suggested oval the developer list are easy and some we will have to think about some more. Since you are wearing two hats, with your work on security guidance and OpenSCAP, your guidance on implementation would be very helpful. We could maybe have a Birds of a Feather session at Developer Days. Your guidance would be great for the OVAL Community.

Steve Grubb: We could focus on how to implement things and collect information from the system.

Jon Baker: We might fit something in if the OVAL agenda allows for it.

Dave Waltermire: We are working to generate SCAP content from DISA Gold Disk checks and our challenges seem to be aligned with Steve Grubb's. Would it make sense to have a developer teleconference early in Version 5.8 to discuss these challenges?

Jon Baker: The reason that we haven't responded to Steve Grubb's emails to the oval-developer-list is because we have been trying to keep everyone focused on Version 5.7. Dave Waltermire, if you have any ideas, please post them to the oval-developer-list. Charles Schmidt and XCCDF have had great success with developer teleconferences, and we can have one if needed, but we would like to see what you have on the oval-developer-list first to see what you are doing with generating SCAP content from Gold Disk checks.

Conclusion

Thank you all for participating in the call, and taking time out of your busy days to attend. Things are going great for OVAL, and we hope to see a lot of you at Developer Days. Reminder, as the Version 5.7 release comes up, we will be pinging all of you for the approval required to make Version 5.7 official.