OVAL Board Meeting (4/9/2012)

Attendees

Anthony Busciglio - Cisco Systems Inc.
Chandrashekhar B - SecPod Technologies
Dave Waltermire - NIST
Eric Walker - IBM Corp.
Jonathan Frazier - Symantec Corp.
Kent Landfield - McAfee Inc.
Aharon Chernin - DTCC
Morey Haber - eEye Digital Security
Noah Salzman - IBM Corp.
Omar Santos - Cisco Systems Inc.
Steven Piliero - Center for Internet Security
Alberto Bastos - Modulo
Steve Grubb – Red Hat Inc.

Jon Baker - MITRE
Matt Hansbury - MITRE
Dan Haynes - MITRE
Jasen Jacobsen - MITRE

Meeting Summary

Welcome

After introductions the group was welcomed to the 2012 2nd quarter OVAL Board Meeting. One new board member was introduced to the group:

Noah Salzman – IBM Corp.

Status Update

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

OVAL Language

Version 5.10.1 became official on January 27, 2012 addressing the missing entity in the linux-def:rpmverifypackage_test, the new three-component version identifier, and other minor changes and clarifications to the OVAL Language documentation. Please see the OVAL 5.10.1 page for additional details about the release.

A working draft of the UNIX Component Model Specification was released on April 4th. A working draft of the Windows Component Model Specification was released on January 19th. With these specifications, we have tried to provide additional information that will make using and implementing the OVAL Language much easier. However, the usefulness of these specifications really depends on

whether or not they contain the information that is needed by the community. As a result, any feedback will be greatly appreciated.

The OVAL Language Sandbox was announced over the oval-developer-list last week. Since, then we have started to develop tests from the artifact hunting use case in the OVAL Language Sandbox. The artifact hunting use case focuses on extending the OVAL Language to better support the detection of malware on Windows platforms and was introduced by the CyberESI team at last year's OVAL Developer Days. We are also still in the planning phase for OVAL 5.11 and would appreciate any thoughts on what you think should be the major focus areas for this release.

OVAL Interpreter

The 5.10.1.1 build of the OVAL Interpreter was released with the 5.10.1 release of the OVAL Language. This build featured the implementation of the linux-def:rpmverifypackage_test, updates for the three-component version identifier, and many other bug fixes and feature requests. Please see 5.10.1.1 build release notes for a complete list of changes. We are now working on the windows_view behavior that applies to the registry and file based tests on 64-bit Windows platforms. These changes are currently available in the windows_view branch.

[Kent Landfield] Has the intent of the OVAL Interpreter changed to fully implement the OVAL Language?

[Jon Baker] The priorities for the OVAL Interpreter have always been to implement the core part of the OVAL Language first (OVAL Definitions, System-Characteristics, Results, etc.), then the key constructs (i.e. high-risk) in the OVAL Component schemas. For example, we implemented the win-def:cmdlet_test because we wanted to make sure that the construct could be implemented before including it in an official release. Are there concerns about the OVAL Interpreter being complete?

[Kent Landfield] I would rather MITRE focus efforts on OVAL Language specification development than attempting to completely implement the OVAL Interpreter. It is one thing to add new capabilities if people are contributing those new capabilities, but, there are vendors that are just using the OVAL Interpreter in their tools as it is.

[Jon Baker] The OVAL Interpreter is an open source project and is freely available under the BSD license that we developed with the OVAL Board. We regularly receive community code contributions for the OVAL Interpreter, and these contributions could easily expand the scope of the OVAL Interpreter work. Of course, we review and test code contributions before integrating them into the OVAL Interpreter and make sure that the contributions align with the goals of the reference implementation. So far, we also haven't come across any contributions that have not seemed to align with the scope of the OVAL Interpreter.

[Eric Walker] OVAL Full Results. Why implement the capability when it is done and works in the OVAL Interpreter? If it gets you into the market, why not use it and fill out the capabilities?

[Kent Landfield] I am on the fence about this because it serves as a useful resource to the community and some vendors are just using it. I just don't want the community pushing this work onto MITRE.

[Eric Walker] Why not just let MITRE decide?

[Jon Baker] This is a good discussion, but, let's schedule a follow up call to further discuss this issue because we have a full agenda for today.

[Dave Waltermire] What was the latest build version and date?

[Danny Haynes] The latest build was ovaldi-5.10.1.1 and it was released on January 27th, 2012.

OVAL Repository

The OVAL Repository's definition count at the time of the call was 13,491. DTCC, G2 Inc., SecPod Technologies, and Symantec Corp. received the Top Contributor Awards for the 1st quarter of 2012 for their submissions to the OVAL Repository. We are also making significant changes and upgrades to the OVAL Repository infrastructure to improve the performance of the infrastructure and the tools used to process community submissions. These improvements will allow the MITRE team to better handle larger content submissions, which currently can stress our tool set and make it difficult to process the content.

OVAL Developer Days Planning

OVAL Developer Days will be held in conjunction with the SCAP Developer Days event from July 9th, 2012 to July 12th, 2012 at the MITRE Corporation in Bedford, Massachusetts. We have requested approximately a half of a day for OVAL-related topics and would really like to see a few vendor-led discussions during the event. If there is a topic that you would like to lead, or if you have any suggestions for topics that should be discussed at the event, please let us know.

OVAL Sandbox Update

The OVAL Language Sandbox provides the community with a common location to develop and share new and emerging capabilities independent of an official OVAL Language release. During the January 9th, 2012 OVAL Board Meeting, we discussed a high-level proposal for the OVAL Sandbox and we were provided with feedback to develop a more concrete version of this proposal. The OVAL Language Sandbox was announced on April 4th, 2012 over the oval-developer-list and represents our first pass at a concrete version of our proposal. Given that the proposal is our first pass, we understand that it may need to change and evolve as the community begins to use it. As a result, feedback on how to improve it will be greatly appreciated.

A high-level overview of the Sandbox Development Process and the Sandbox Migration Process was also given. Please see the OVAL Language Sandbox page for more detailed information about these processes.

[Dave Waltermire] Have you considered the Sandbox as an incubator for the OVAL Language and the community would select items from the sandbox to move into the next release?

[Jon Baker] We need to learn through experience based on what people submit to the sandbox and how it evolves. Do others have ideas for extensions that they would like to develop in the OVAL Language Sandbox?

[Steven Piliero] We have content that will require extensions to the OVAL Language and would be willing to develop it in the OVAL Language Sandbox. Some of these things are more long term capabilities. We would also like to add scripting.

[Kent Landfield] I would like to see some work on making extensions in the network management space.

[Dave Waltermire] I would like to see the exploration of network devices (e.g. NETCONF, SMNP, etc.).

[Kent Landfield] I would also like to see improvements to our current database capabilities.

[Dave Waltermire] I think work in the scripting area would be good too.

[Stephen Piliero] Databases are a pain point for us too.

[Jonathan Frazier] When we get into scripting and databases, we need to be cautious of malicious injection via content. Security content should not open security holes.

[Danny Haynes] When we developed the win-def:cmdlet_test, we utilized schema restrictions and constrained run-spaces to protect against the use of malicious security content and injection. This is a very good thing to keep in mind when moving into these areas.

[Dave Waltermire] Have you considered a build or test harness for content in the sandbox? Are there documented conventions for creating a build?

[Danny Haynes] In the OVAL Language Sandbox wiki, we have a page on conventions to use when developing new constructs such as what to name the experimental schemas, namespace, etc.

[Dave Waltermire] I was more thinking of automated building and testing.

[Danny Haynes] No, we really haven't thought much about that.

[Jon Baker] We really see this as a first step and wanted to develop conventions early so that we could use them, adjust them, and make sure they work. However, we expect to learn through a bit of usage and that learning will evolve our approach and usage of the sandbox.

[Eric Walker] Have you considered going in this direction with the OVAL Repository content?

[Jon Baker] The sandbox is our first try at this and we could see over time moving other aspects of the project (e.g. OVAL Interpreter, Test Content, Official OVAL Language Schemas, etc.) over to GitHub, but, we want to make sure we get the process down. I could see the OVAL Test Content being transitioned over in the near term, but, I think the OVAL Repository content would be a bit further down the road.

OVAL and Mobile Devices

We have received requests for OVAL extensions for mobile devices including IPhone OS and Android. In response to these requests we have spent a small amount of time looking into extending OVAL for Android. In doing so, we found that since Android is a UNIX-based operating system it would probably

be best to focus on taking the existing constructs, such as those from the UNIX, Linux, and Independent schemas, and implementing the constructs that are applicable. From there, it would then make sense to move onto Android-specific capabilities such as adding a test for checking information about Android application package files (APK) which are like RPMs for some Linux systems. Once a core set of capabilities is established, we could then develop targeted sample content that would demonstrate the capabilities on the Android platform.

We wanted to spend some time discussing this to raise awareness as an emerging need for the OVAL Language and wanted to offer that we would be glad to work with the community in this area to develop it in the OVAL Language Sandbox and the OVAL Interpreter.

[Steven Piliero] I agree with some of things mentioned about Android, however, I would like to see what the biggest pain points for the community are and focus on those things. That way we can focus our efforts on those that have the most impact.

[Jonathan Frazier] I agree with that, but, most businesses use IPhone now and I don't think Android would be as big of a deal from a commercial perspective.

[Dave Waltermire] What is the lowest hanging fruit? Have you considered looking at management platforms? You may not want to assume that mobile device assessment will occur on the device.

[Jon Baker] No, but, I agree that is a good point.

IETF SACM Recap

Lastly, Kent Landfield led a recap on the IETF SACM side meeting that was held at the IETF 83 Meeting in Paris, France. Many members of the international community want to participate and adopt the standards, however, they are hesitant because they currently see them as U.S. Government standards and would like them to be transitioned to an international standards body. We have seen significant interest by the Japanese, French, and Australians.

The purpose of the SACM side meeting was to begin getting a working group started and showing that these standards are more than just U.S. Government standards. We need to figure out how to shift some of the current standards work to the IETF and continue development of these efforts and new efforts in the IETF.

Another key thing about the IETF is that you don't need government support. You just need people to come together to solve a problem. By participating you can be an early adopter and influence the direction of the work.

We are currently looking at what standards we have and how we can get people involved. We are also working on a use case document and the first draft should be available by the end of April. The use case document is currently being developed over the SACM mailing list.

[Dave Waltermire] I sent a link to sign up to the SACM mailing list to the oval-board-list for anyone who is interested.

[Jon Baker] Since we are out of time, we should continue this discussion in a follow up call.

Action Items

- Follow up call to further discuss the IETF SACM effort
- Follow up call to further discuss the role and development of the OVAL Interpreter
- Survey the community for major trouble areas for awareness and to help coordinate sandbox development
- SACM follow up email describing the relationship between OVAL and various IETF efforts. This message will include SACM side meeting slides and minutes.