OVAL Developer Days

July 11-12, 2006

Introduction

OVAL Developer Days was held on July 11-12, 2006 at The MITRE Corporation in Bedford, MA. The purpose of this event was to focus on the recently released version 5 of the OVAL Language and to educate attendees about the new features that have been added. In addition, other areas of concern (repository, compatibility) were discussed in an attempt to improve the associated procedures and requirements. By bringing together the lead proponents within the OVAL Community, the goal was to derive solutions that would benefit all parties, and continue the development of the language. What follows is a detailed summary of the discussions from this event.

Please refer to the presentations that were given for additional information. They are available on the OVAL Web site.

Attendee List

Assuria	-	Chris Wood
BigFix	-	Anna Min
CA	-	Mark Gergely
	-	John Devereux
Center for Internet Security	-	Dave Waltermire
Citadel Security Software, Inc.	-	Kent Landfield
Configuresoft, Inc.	-	Dennis Moreau
	-	Greg Frascadore
Department of Defense	-	Melissa McAvoy
Mindjet	-	Nils Puhlmann
MITRE	-	Margie Zuk
	-	Dr. Todd Wittbold
	-	David Mann
	-	Charles Schmidt
nCircle	-	Michael Murray
	-	Jay Graver
	-	Mike Luu
NIST	-	Steve Quinn (telecon)
	-	Peter Mell (telecon)
	-	Richard Ayers
PatchLink Corporation	-	Tom Klemzak
	-	Ken Lassesen
Secure Elements	-	Scott Carpenter
	-	Andrew Bove
	-	Dave Neimoller
ThreatGuard	-	Rob Hollis
	-	Randy Taylor
University of Nebraska at Omaha	-	Matt Payne
OVAL Team	-	Steve Boczenowski
	-	Matt Wojcik
	-	Jon Baker
	-	Andrew Buttner
	-	Dr. Harvey Rubinovitz
	-	Bob Martin

Day One

Session 1

OVAL Tutorial

OVAL Developer Days opened with a tutorial on version 5.0 of the OVAL Language which was released on July 16th, 2006. Topics included the breakout of <objects> and <states>, the use of variables within OVAL, complex objects involving <sets> and <filters>, and definition extension. A simple 'Hello World' example was stepped through to help demonstrate writing content in the new format.

Overall the session was about educating the attendees, so discussion was limited to questions about some of the material. One of the nicest comments at the end of the session was about how all the topics discussed at last year's OVAL Developer Days seem to have been addressed in the new version. The entire presentation is available on the OVAL Web site.

Session 2

The second session focused on the OVAL Repository. Some background information was presented about the goals of the OVAL Repository, followed by an outline of its history. The details of this talk can be found in the presentation available on the OVAL Web site. Discussion at the end of the briefing was focused on the future direction of the OVAL Repository.

External Repositories

There was some discussion on how external repositories fit into the OVAL Community. Currently, Red Hat hosts an external repository containing patch definitions for their security advisories. Our hope is that additional OS vendors will stand up external repositories to cover their operating system.

If this becomes reality, how should the OVAL Repository relate to these external repositories? Should the content held in an external repository be copied into the OVAL Repository? Or should the OVAL Repository link to the individual definitions held in the external repository? Both of those suggestions involve incorporating the external content in the OVAL Repository and hence subjecting them to the community review process. It was then mentioned that when dealing with patch content, OS vendors are the definitive source and they should not be subject to the community review process. In addition, pulling in content from external repositories opens up the challenge of keeping both repositories in sync and up to date. Another suggestion is to simply provide links to the external repositories as a whole. In essence notifying users about them and providing a source for the OVAL Community to find the different external repositories that are out there.

It was also pointed out that the type of content being produced factors into the decision. Patch content is more likely to be taken directly from the OS vendor, while vulnerability or configuration content might be better served by the community and the review process.

A feature to the language that could help with the relationship between external repositories was discussed. Currently in version 5.0, any OVAL Definition linked to by an <extended_definition> tag must reside in the definition document. The proposal is to have an <external_definition> that is just a reference to a definition located in some external repository. The id and location of this definition would be provided so tools can fetch the definition during evaluation. This allows extension of other's content without forcing the definition writer to pull in

all the content they are extending. Note that XML Includes could be used with the current schema to accomplish something similar.

Inventory Definitions

With version 5.0, definition extension allows content writers to make better use of inventory definitions. Discussion ensued about how inventory definitions should be supported in the OVAL Repository. Correct use of inventory definitions should reduce the amount of maintenance as changes will only need to be made in one place. Of course a collection of inventory definitions needs to be developed in order for them to be used. This is an area of work for the community over the next couple of months.

Content Writing

Support for content writers needs to be improved. Suggestions included adding functionality to the OVAL Web site to allow searching for all the definitions that include a specific OVAL Test. This feature will help provide an understanding of where a certain test is used if a modification needs to be made. Another feature that would be of great help would be the ability to determine if a specific <object> (or <test> or <state>) already exists so that it can be reused.

Another area to help with content submission is a tool to detect when duplicate tests/objects/states are being submitted. Basically it would flag something as already in the repository and give the id so the content writer can make the modification.

It was also mentioned that a schema for validating the metadata required by the OVAL Repository (as opposed to the metadata required by the OVAL Language) should be available to assist content writers.

Definition Documents

It was requested that the OVAL Community have more flexibility in creating the definition documents (for example, a definition document containing all the Windows XP definitions) that can be downloaded from the web site. In an ideal world, the user could enter a set of criteria (similar to the search criteria) and a definition document based on this would be created and available for download.

Schematron Validation

One way to help validate the content that is being submitted is to utilize the Schematron statements that have been bundled into version 5.0 of the OVAL Language. This should become a requirement for submission as it will help catch a number of small errors that commonly occur.

Discussion

In between sessions, a discussion was held regarding the breakup of OVAL Definitions pertaining to the issue they are defining. For each issue (a vulnerability, or a patch, etc.), should only one OVAL definition be written? Or should multiple smaller definitions be written, each defining a specific platform?

The discussion led to the idea of having a number of individual definitions focused on specific platforms all wrapped up by a single definition that extends the individual definitions to define the issue in its entirety. This approach would have the problem of having two OVAL ids associated with each issue.

Does writing only one OVAL definition per issue imply completeness? A definition writer might not have the knowledge to write the definition for every system, either not knowing how to, or not having the schema for additional platforms. When evaluated, the answer that is given is assumed correct and a user will think they are not vulnerable when in fact they very well could be. This problem could be solved by the correct use of the

<unknown_test>. If a definition writer knows that a certain platform is affected, but is unable to write the OVAL piece for it, an <unknown_test> can be written to say this. That way, evaluation of the OVAL Definition will result in "unknown".

Another issue with breaking up a definition is that the breakup becomes inconsistent across different definition writers. Some writers choose to break up the OVAL definitions one way, while others choose to break things up a different way. It is hard to enforce this even with a documented style guide. It is much easier to get the community following a consistent format with one definition per issue.

Overall, the room was split on this topic and further discussion should be had.

Session 3

Automated Security Measurement

Steve Quinn and Peter Mell of NIST presented on their work involving FISMA Technical Control Automation. They are working with OVAL and other standards including XCCDF, CVE, and CVSS in an effort to express security guidance in a machine readable automated way. Please look at the presentation available on the OVAL Web site for more information.

Day Two

Session 4

The forth session was focused on OVAL Compatibility. After a quick introduction to the compatibility program, a number of edge use cases were presented. For each one, we discussed whether the organization/individual should be part of the compatibility program. These use case discussions themselves were meant to start conversations regarding the direction of OVAL Compatibility and led to a number of additional topics.

OVAL Supporter

There are a number of use cases that don't fit exactly into the defined OVAL Compatibility program. These capabilities should still be recognized and this can be accomplished through the OVAL Supporter section. An OVAL Supporter is a capability that incorporates OVAL in some way, but yet does not fit the model of OVAL Compatibility. OVAL Compatibility should be limited to those tools that exchange information in the OVAL format.

OVAL Certification

In addition to having the compatibility program for capabilities (tools and services), the idea of an OVAL Certification process for individuals was discussed. In order to be a certified OVAL contributor, an individual would need to pass a test. Creating such a test would be a difficult task and administrating it would be an even tougher task. Even with these challenges, this would provide a foundation to build upon. By certifying individuals, it gives organizations a way of verifying who has at least been exposed to OVAL.

OVAL Certified individuals would not be required for a capability to achieve OVAL Compatibility (or vise versa) OVAL Certification would just be a way to distinguish who an organization has on their team and represent some level of expertise in the OVAL arena.

Primary Source Vendors

An idea for promoting creation of content and for rewarding those vendors who produce OVAL Definitions is to establish the notion of Primary Source Vendor and to call them out with a special award / distinction. This might help provide incentive for those vendors that are not currently participating. This title would be a special tag given in addition to OVAL Definition Producer.

These different labels within compatibility allow customers to more effectively search for the specific product they are looking for.

We could take this a step further and also have an Authoritative Source classification. The big challenge here would be determining who the authoritative voice is.

Session 5

OVAL Extensions - <remedy> and <solution>

Ken Lassesen from PatchLink gave a presentation about the need for remedy and solution information within OVAL. He had submitted a proposal to the OVAL Community before OVAL Developer Days regarding a technical implementation of <remedy> and <solution> tags. The presentation was geared at getting the ball rolling in that direction. Please look at the presentation available on the OVAL Web site for more information.

It was noted that there might be some overlap with features already in existence with XCCDF. XCCDF can be used to define policy level decisions. An example would be trying to determine which alternative to choose. Going forward we need to investigate how XCCDF might help provide some of the needed functionality.

Session 6

The final session of the day was a talk regarding XCCDF-P. This is an NSA led effort that has been in the works for about a year. Its main goal is to define a data model and XML representation for expressing qualifications and hierarchies of facts about platforms. This effort is related to OVAL in that OVAL definitions have a need to express which platforms they are intended for, currently accomplished through the <affected> element. In addition, OVAL inventory definitions can be written for each defined XCCDF-P identifier.

XCCDF-P - Three Part URN

The latest proposal for XCCDF-P is to break the URN identifier into three distinct parts: a hardware part, an OS part, and an application part, with each part being optional. The goal would be for the identifier to represent a class of machines that match the characteristics held within the id, thus allowing policy to be associated with those machines. The URN is not meant to be a complete description of the system but rather a way to identify a class of systems.

The format of the URN would in essence be three small hierarchies, one for each part. The hierarchy structure allows higher level classifications to be assumed. The original XCCDF-P format was based on a similar hierarchy and there were questions about how effective a hierarchy can be at covering the vast array of platforms in existence. Breaking the single hierarchy into three smaller hierarchies has not solved the problem completely, but has enabled it to more easily identify a wider range of complex platforms.

Conclusion

Thank you to all that attended and made OVAL Developer Days 2006 a great success. The OVAL team is looking forward to working with everyone to expand on the topic discussed and come to a conclusion on many of the issues presented. See everyone next July!!