OVAL Board Meeting (10/15/2012)

Attendees

Scott Armstrong – Symantec Corporation
Chandrashekhar B – Secpod, Inc.
Carl Banzhof – Rockport Systems
Anthony Busciglio – Cisco Systems, Inc.
Blake Frantz – Center for Internet Security
Steve Grubb – Red Hat Inc.
Rob Hollis – ThreatGuard, Inc.
Kent Landfield – McAfee, Inc.
Adam Montville – Tripwire, Inc.
Steven Piliero – Center for Internet Security
Noah Salzman – IBM Corp.
Omar Santos – Cisco Systems Inc.
Amaresh Shirsat – Symantec Corporation
Randy Taylor – ThreatGuard, Inc.
Tim Keanini – nCircle Network Security, Inc.
Eric Walker - IBM Corp.
Dave Waltermire – NIST
Chris Wood – Assuria Limited

Jonathan Baker – MITRE
Matt Hansbury – MITRE
Danny Haynes – MITRE
Michael Cokus – MITRE
David Rothenberg – MITRE

Meeting Summary

Welcome

The group was welcomed to the 2012 4th quarter OVAL Board Meeting.

Status Report

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

OVAL Language & Interpreter

The OVAL team has recently released Version 5.10.1.3 of the OVAL Interpreter. This build adds support for the ind-def:environmentvariable58_test, the language entity in the win-def:file_test, the has_extended_acl entity in the unix-def:file_test, the last_login_time entity in the win-def:user_test, the last_write_time entity in the win-def:registry_test, and the windows_view behavior for file tests in the 32-bit version of the OVAL Interpreter. It also includes various bug fixes.

OVAL Adoption

OpenVAS and the National Institute of Advanced Industrial Science and Technology (AIST) were recently recognized as Official OVAL Adopters and DISA Field Security Operations (FSO), Lunarline, and GCP Global made declarations to support OVAL in their products. DISA FSO and Cisco were also listed as “Other Repositories” of OVAL content. Cisco’s repository features OVAL definitions and CVRF content alongside their security advisories for IOS.

OVAL Repository

A quick update for the status of the OVAL Repository was provided. The OVAL Repository's definition count at the time of the call was 13845 definitions. The 3rd quarter's top contributors were G2, Inc. and SecPod Technologies.

Main Topics

The main goal of this Board call was to outline planning for an OVAL 5.11 release and begin a discussion of the OVAL Interpreter license. The OVAL 5.11 release discussion included taking a look at the capabilities currently in the OVAL Sandbox, proposing possible release goals, and querying the Board for their list of priorities. Possible focus areas for the release include extending OVAL to new platforms such as mobile devices, incorporating improvements and new capabilities for network devices, and expanding the OVAL Language to improve support for complex file formats and file system searches.

Why a Next Release?

Since the introduction of the OVAL Sandbox, there have been several new capabilities that have had schema, content, and a working prototype provided. These capabilities may be mature enough to consider for inclusion in an official release of the OVAL Language. There are other less mature capabilities in the Sandbox that may also be considered. The OVAL Specification is due for an update and could be further simplified. There are also several open bugs and miscellaneous feature requests that could be addressed. The Board was asked to consider several topic areas and shape the release contents based upon what they are hearing from their end users and seeing in industry.

Discussion

Kent Landfield shared that he was getting asked for additional Cisco network support and that he is increasingly being asked to support network infrastructure rather than host-based systems. He had also discussed the mobility area and how there was the question of whether to go with OVAL or another interface. It was Kent's wish to push for advancement within OVAL in this area so that it may help prevent it from being superseded.

Adam Montville added that he too was looking for increased Cisco network infrastructure support. He had not been asked by customers about the mobility area so networking was his top priority.

Omar Santos commented that Cisco had made lots of changes to their IOS schema. He added that there will soon be an initial schema for Cisco IOS XE, IOS XR, and NX-OS. It was agreed by all that the incorporation of these component specifications should be a priority.

Mobile Devices

Mobile device management is an area that is gaining more and more attention. It was suggested that OVAL should adopt the Android schema in the OVAL Sandbox. This extension would provide an immediate starting point since it had a schema, content, and a working prototype and clearly demonstrates to the mobile device security community that OVAL can be applied to Android. The schema may need revisions later on as we learn, but the schema today represents a significant opportunity. If OVAL is unable to demonstrate applicability to mobile devices, other data formats will necessarily fill in this gap. It was asked of the Board whether they thought it may be mature enough to include in the OVAL 5.11 release. It was also asked whether there should be a focus on Android, or if we should also seek to include Apple's iOS.

Discussion

Kent Landfield suggested that it would be better in the long run to do things the "right way." This would involve having someone reach out to Google to see if we can interest them in verifying or validating the existing schema, and possibly count on their participation. He also made the point to focus only on Android for now. Given the multiple OSes in the marketplace, it would be easier to start with the open system. This would raise awareness and possibly prevent duplicated efforts. As this develops, it could also get Apple interested in participation.

Tim Keanini suggested that he could provide contacts within Google to launch this effort.

Cisco Updates, JunOS, NETCONF

The topic of OVAL for network devices was brought up to show where we are currently at and where we may proceed. Two Board calls ago, members had expressed an interest in the YANG modeling language and the SNMP protocol. It was asked whether anyone had any interest in developing those capabilities in the OVAL Sandbox. Schemas for Cisco, Juniper, and NETCONF are currently in the Sandbox and the Juniper and NETCONF schemas have a working prototype as well. The Board was also asked whether there may be anything else related to network devices as well as their thoughts on the current Sandbox capabilities.

Discussion

David Waltermire asked for examples of specific support for the management protocols whether it be NETCONF or SNMP. Jon Baker was able to direct him towards the 2012 MITRE Developer Days where the NETCONF schema was shown and a demo was given, though cautioned that this was a work in progress and the community was not sure that it was needed in the OVAL Language.

Jon followed up by asking for more input on whether anyone has experimented with SNMP, YANG, or others and pointed out that a NETCONF schema was drafted in the Sandbox. These are additional areas that can be considered if the community is willing to verify the need for such extensions.

Kent Landfield shared his views that of the three major network device vendors (Cisco, Juniper, and Alcatel), only Cisco and Juniper have been actively engaged in contributing OVAL extensions for their platforms. If the next release includes solid support for Cisco and Juniper platforms, OVAL will have made significant progress in network device support.

Steve Piliero mentioned that the top three network device vendors he hears about are IOS, ASA Firewall Services Module, and XOS, but that he also hears about HP support.

Adam Montville has heard requests for HP and Dell.

Artifact Hunting

Artifact hunting is still a priority for OVAL to support, but MITRE is not currently in a position to make significant advancements in this area. MITRE will look to ensure that any of the low hanging fruit that has been proposed by the community is addressed in the next release, but will likely not have the resources to do significant development in support of this use case. The board was generally supportive of this.

Database Vulnerability Assessment

The IBM InfoSphere Guardium Team presented at the 2012 MITRE Developer Days where they discussed problems and improvements to the sql57_test. The OVAL Team is currently implementing the sql57_test in the OVAL Interpreter to drive community discussion. The Board was asked whether there were other concerns with this test and whether improvements to this test were still a priority.

Discussion

Jon Baker commented that we were working on the test primarily to get more experience with it, and wants to ensure that a 5.11 release will support the database assessment use case.

Kent Landfield commented that the test still needs work. As it stands with the current security issues, they do not seek to implement it. Customers are still asking about the sql test and any work that gets done would be appreciated.

Dave Waltermire suggested enumerating the critical issues for the sql test.

Eric Walker wished to reach back to the IBM InfoSphere Guardium Team for feedback on security issues. He wanted to make sure, however, that taking on database-related functionality would not push aside other important work.

Jon Baker responded that this was a simple implementation, and that since it was being agreed upon as higher priority than the artifact hunting use case, this would take precedence. Jon reminded the group of the 2012 Developer Days discussion on database assessment and Danny Haynes agreed to resend related material from Developer Days to the Board.

Dave Waltermire expressed interest in coming up with a checklist for the Board to document what would be in the next release, prior to approval.

Jon Baker commented that much of this documentation already exists, but has yet to be presented to the Board. He wishes to focus on the release and let that reveal the individual priorities. He wishes to keep the dialog open with the OVAL Board to cover items as they may arise over the year. Jon would also like to get the goals documented, and present this to the OVAL community as well to gather their input.

Improving Support on Apple Products

With the announcement of the SCAP-On-Apple project at macosforge.org, Shawn Geddis has shown that Apple is willing to provide domain expertise on Apple products. The recent BOF meeting at the 2012 ITSAC yielded good attendance, which shows others are interested in helping.

MITRE will look to this group for guidance in advancing OVAL's support for Apple products. The plist_test has undergone 3 iterations and needs to be finalized and there was a request to add a pkgutil_test. A primary goal should be enabling the full automation of Apple Security Guides and STIGs for Apple OSX and iOS. The Board was asked if they had similar priorities with supporting Apple OSX and iOS as they did with Windows and Linux, and if there were specific areas that need improvement.

Discussion

Kent Landfield agreed the Apple platform support definitely needed improvements.

Jon Baker was hopeful that the OVAL community would be able to take advantage of Shawn Geddis' support and the activity within the new open source project to finally have solid Apple product support in OVAL. Development in this area will be largely dependent upon the contributions from the community and the new Apple hosted project.

Searching File Systems

A brief overview of the challenges with searching file systems was presented. Listed among the worries are the ongoing confusion with symbolic links and treating paths as case-sensitive strings. The OVAL

Specification needs to clarify these in order to simplify the language. Board members were invited to share their views on the current/future state of directory traversal.

Discussion

Kent pointed out that additional optimizations to make file searching more efficient would be desirable.

Steve Grubb commented that file containers are about to become more prevalent on Linux distributions, and that a mechanism like chroot will likely be required to properly check them.

Complex File Formats

MITRE is increasingly asked to expand OVAL's current text and xml file content tests to better support other well-known configuration file formats. In most cases today, an author must attempt to use one of the file content tests, however this is insufficient when trying to examine highly structured files. Some examples of types that the OVAL team has been asked about include php, binary, and apache config files. The Board was asked to what extent we should focus on this, and if we should limit it to only the more widely known formats.

Discussion

Steve Grubb expressed a desire to see a specialized test be able to examine Java JAR files. These files may need to be unzipped to a temporary directory, and then examined to review their indexed dependencies.

Danny Haynes replied that initially it seems like it would alter the state of the machine, which is something we try to avoid while using OVAL. It would be looked into further.

OVAL Licensing

Jon Baker provided a brief history of the selection of the current OVAL license. It was selected with the Board with Version 4.0 of the OVAL Language. Since changing the license would be seen as a major act, Board members were asked to provide a compelling reason to do so. This topic had begun shortly before the end of the Board call, and did not provide adequate time to discuss.

Discussion

The Board was asked if they would be able to attend a follow-up call on Friday 10/19 to further discuss the OVALDI licensing issue. Most Board members confirmed that Friday 10/19 would be an acceptable date for the follow-up call.

Conclusion

The call provided great discussion about the desires of the OVAL Board to expand OVAL, and gave good direction on how to proceed. However, not all topics were discussed including scripting, OVAL core issues, open discussion for any areas that we may have missed, and developing a release timeline. It was decided that these topics could be further discussed over email.