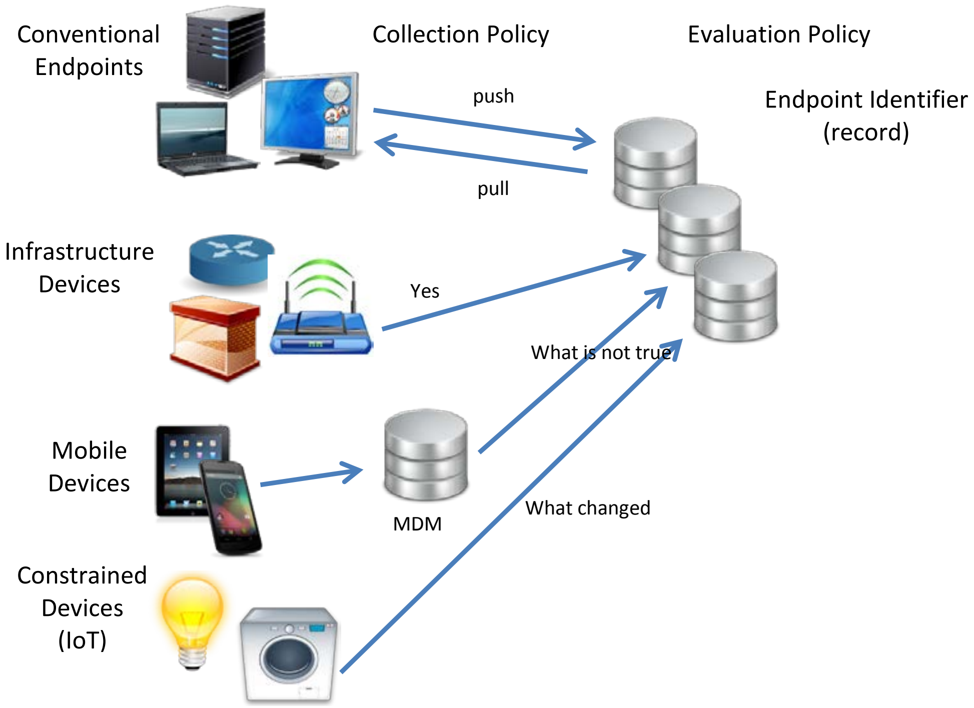
Change in Operational Model for OVAL

Over the past two years, the security automation leadership within the US Government (DHS, NIST, and NSA) has been developing a long-term strategy for security automation that focuses on sustainability and scalability. Specifically, this strategy focuses on working with the security automation community to take the lessons learned over the past decade to evolve SCAP and its component specifications, leverage additional capabilities such as Software Identification Tags (SWID) and Trusted Network Connect (TNC) protocols, and develop new capabilities where there are gaps. We are working to shift to a model where the authoritative primary source vendor provides the required data and to use standardized protocols, interfaces, and schema to collect the necessary data from endpoints. This strategy directly aligns with the work currently being done in the IETF Security Automation and Continuous Monitoring (SACM) working group and TCG TNC working group.

In conjunction with this strategy, MITRE's sponsor for OVAL, Federal Network Resilience (FNR) within DHS, is changing the model by which OVAL is operated. Effective immediately, OVAL will no longer be operated under an independent third party model with the DHS sponsor taking on an active, directional role for the project.

What Does this Mean for OVAL?

Simply put, OVAL must evolve to align with the US Government security automation strategy. This strategy separates the collection of endpoint software inventory and configuration data, and the evaluation of that endpoint data against some policy. This places emphasis on the ability of endpoints to publish their configuration data to a centralized content management database among other things. It also targets a wide array of endpoints types which can be categorized into one or more of the following: conventional endpoints, network infrastructure endpoints, mobile endpoints, and constrained endpoints. A simple diagram of this architecture is presented below.



While the current design of OVAL largely supports this, there are still some interdependencies between collection and evaluation that need to be addressed. More critically, this represents a shift in how OVAL has traditionally been used where third-party security tools report the assessment results of an endpoint to one where the authoritative sources for software running on the endpoints publish configuration data to a central location where the assessment is performed. To accommodate all of this, OVAL must be more discreetly separated into its major components (OVAL Definitions, OVAL System Characteristics, and OVAL Results). Additionally, these different components must be considered with respect to how they fit into the SACM architecture and what gaps must be filled to further evolve the Language.

Direct Impact to OVAL

- **Version 5.11** - MITRE will continue the OVAL 5.11 release under the current model for features that are currently in queue (i.e. features that are in the OVAL Sandbox and scheduled for an OVAL Board vote). DHS sponsor approval will be required for any additional capabilities and will be determined based on the level of effort, need, and impact of the capability.
- **Future OVAL Releases** - MITRE will not actively develop an OVAL 5.12 release. However, MITRE will be working with the DHS sponsor to determine the best way to handle critical additions to the Language, with ideas such as a limited 5.12 version (or additional subsequent versions) and a move towards unofficial extensions as possible options.
- **Future Work** - MITRE will shift its focus to support work by government participants in the IETF SACM WG under the direction of the DHS sponsor.
- **OVAL Adoption** - MITRE will move away from active outreach with respect to OVAL in order to focus on the advancement of the US Government security automation strategy.
- **OVAL Repository** - MITRE will continue to process OVAL Repository submissions until a suitable transition strategy can be developed and executed. MITRE will look to the community and work with the DHS sponsor to determine how best to transition the ongoing moderation of the OVAL Repository.
- **OVAL Interpreter** - No additional development and maintenance will be undertaken on the OVAL Interpreter after the OVAL 5.11 release under the DHS work program. As an open source project MITRE will continue to accept community code contributions. However, MITRE will likely look towards the community for a new open source project lead.

OVAL Board Meeting (4/14/2014)

Attendees

Blake Frantz – Center for Internet Security
Chris Wood – Assuria Limited
Dave Waltermire – NIST
David Solin – jOVAL.org
Jack Vander Pol – SPAWAR, U.S. Navy
Jamie Cromer – Symantec Corporation
Kent Landfield – McAfee, Inc.
Randy Taylor – ThreatGuard, Inc.
Scott Armstrong – INADEV Corporation
Steve Grubb – Red Hat Inc.
Tigran Gevorgyan – Qualys, Inc.
William Munyan – Center for Internet Security

Jonathan Baker – MITRE
Matt Hansbury – MITRE
Danny Haynes – MITRE
David Rothenberg – MITRE
Luis Nunez – MITRE

Invited Guests

Kim Watson – DHS
Melanie Cook – NIST

Meeting Summary

Welcome

The group was welcomed to the 2014 2nd quarter OVAL Board Meeting.

OVAL Direction

The call began with the introduction of Kim Watson from the Federal Network Resilience (FNR) group within DHS, who began by announcing a change to how MITRE operates the OVAL project. At the US Government's direction, MITRE has long operated OVAL as an independent third party. More recently, representatives from DHS, NIST, and NSA, have been meeting regularly and have come to a shared vision for the US Government's security automation strategy which closely aligns with the work being done by the IETF Security Automation and Continuous Monitoring (SACM) working group[1], in which several OVAL Board members participate. As a result, MITRE will no longer operate OVAL as an

[1] http://datatracker.ietf.org/wg/sacm/charter/

independent third party, but will instead operate the project under the direction of DHS in order to focus on and help realize this new security automation strategy[2].

The shift in MITRE's role will not disrupt any current efforts towards the OVAL 5.11 release; MITRE will continue in its current role for the remainder of the OVAL 5.11 release. From that point on, MITRE will work under the direction of the DHS sponsor to address any critical gaps found in the future by either publishing a targeted OVAL 5.12 release or shifting towards unofficial extensions. Notable aspects of the project which would be affected include the OVAL Adoption Program, which will shift to focus on the advancement of the US Government security automation strategy, and the OVAL Interpreter, which will cease active maintenance after the OVAL 5.11 release. MITRE will shift to support DHS and the wider US Government in engaging international standard organizations, specifically the IETF SACM effort, in order to ensure that work in these organizations aligns and supports a shared vision. The DHS Sponsor is committed to engage the OVAL Board for feedback as this new security automation vision is evolved and made more publicly known.

To aid in the alignment of OVAL with this security automation vision, MITRE will review how OVAL can support a model where software publishes its state to a central database. This model has always been supported by OVAL, but additional work will be required to achieve truly scalable, enterprise solutions. MITRE will also work to understand how the existing components of OVAL fit into the IETF SACM architecture. Specific goals for future documentation include how to make unofficial extensions to the OVAL Language without the help of MITRE. Following this introduction, the Board was invited to share any potential concerns and ask questions.

One OVAL Board member voiced his opinion about the potential for a perception problem if not executed carefully. As a vendor, his concern was that the high level of effort they have placed in promoting OVAL as the leading endpoint checking language would be lost if this new direction was not presented in a transparent and public manner. He pointed towards the increase in overseas contributions to the OVAL Repository as well as other dynamics that should be taken into account. His position is that if they are unable to sell OVAL products overseas, then they would be forced to stop supporting OVAL. Kim responded that under the new security automation vision, transparency, augmented by clarity and unity of direction is of the utmost importance moving forward. This shift is not meant to polarize the OVAL community and may require additional messaging for those who do not feel that they are part of the OVAL community. She continued to assure the Board that no change being made is with intent to derail previous efforts of fostering the OVAL community. There was agreement among the OVAL Board that if this is properly executed, then there is no large foreseeable impact to the future of OVAL.

A second OVAL Board member was concerned about primary source vendor's going back to proprietary checks and agreed with the previous OVAL Board member's concern regarding overseas contributions.

Another OVAL Board member raised a question regarding the desired shift towards a publish model. He asked whether the traditional model of collection and evaluation on the endpoint would go away and be

[2] See pages 1-2 of this document.

replaced by the publish model. Kim’s response was that both methods of evaluation and collection would have their own use cases and likely be used in conjunction with each other. While there will remain a use case for endpoints executing both collection and evaluation and reporting the results, for large enterprise-scale deployments, the separation of collection and evaluation is critical. It will also be critical to push the responsibility for publishing configuration data onto the primary source vendors. The OVAL Board member then noted that OVAL was always designed with having primary source vendors be responsible for their extensions and content, but, that it hasn’t had a lot of support so far leaving 3rd parties to fill in the gaps and asked whether or not there has been any interest from primary source vendors so far. It was noted that NIST has seen some interest from primary source vendors.

One OVAL Board member then suggested that the US Government needs to describe and document specifics so that the OVAL Board can help with this effort and asked about the expected time frames and constraints for this plan. Kim suggested that there would be no issue through November and potentially extended into July of 2015. By then, the sponsor hopes that MITRE would be successful in demonstrating that the pieces of SCAP could be brought before the IETF. Dave Waltermire of NIST responded with further details of an interagency group identifying scalability and sustainability gaps within SCAP 1.2. The majority of the issues they are seeing revolve around expansion to more platforms, ability to get more content, and better product identification. This year they are focusing on software inventory challenges. He pointed to the current ISO work surrounding SWIDs, and the Trusted Computing Group’s (TCG) protocols. He said that it would be tough to establish a timeline for the next iteration of SCAP as they expect SCAP 1.2 to be around for some time, on the scale of years. Dave Waltermire tied the timeline to progress in international efforts, and that it would likely be 2-3 years before enough specifications are made available to change NIST Special Publication 800-126. It is NIST’s goal to have the next version of SCAP be tied to international standards. Kim Watson also suggested that the Continuous Diagnostics and Mitigation[3] (CDM) effort could encourage vendors to speak in standardized ways and that they could potentially be used to find solutions, improve quasi-standards, and provide feedback. Dave Waltermire also noted that the National Cybersecurity Center of Excellence[4] (NCCoE) wants to drive the development of standards and solutions as well as demonstrate the solutions to the cybersecurity community.

One Board member expressed his gratitude that there is a push to an international standards developing organization (SDO). He questioned whether the new sponsor would be funding MITRE to shift OVAL to such an SDO. The sponsor’s response was that with the OVAL Language consisting of multiple parts, there would be required documentation to figure out how it may best fit into the new model. MITRE would be funded to use their expertise to prepare for such a transition.

The same member also voiced concern that the security automation strategy shift could result in more GOTS products, which would undermine his largely commercial customer base. His concern was that there would not be an adequate channel for vendors to provide feedback that they are hearing from their customers. Kim reassured him that the new direction would have feedback channels open at every

[3] http://www.dhs.gov/cdm
[4] http://csrc.nist.gov/nccoe/

step. She wishes to host several events and see how effectively they can receive such feedback. Kim requested that, if at any stage, members felt unheard that they communicate this to DHS so that the feedback loop could be repaired. It is their goal to include the Board the whole way to guarantee they have something viable for everyone. Dave Waltermire added that they do not have specific dates for those workshops but it is something they are committed to going forward.

Next, another Board member pointed out that OVAL's current architecture could support this without needing to completely revamp it and that the missing piece is defining protocols and what level of interoperability is needed (e.g. end-to-end, etc.). They also mentioned that they would like to hear how this impacts the SCAP Validation Program. Melanie Cook who leads the SCAP Validation Program at NIST explained how we need to be sure to include messaging that SCAP 1.2 is not going away and this is more of an evolution and that we want vendors to plan for this evolution.

Another question asked about the SCAP Validation Program, noting that there are a few vendors out there that are in SCAP 1.2 Validation, and a few that are evaluating whether they may get by with SCAP 1.0 or SCAP 1.1 Validation. His concern is that without as many SCAP 1.2 Validated products, transition to an SDO could result in an extended confused state. Melanie Cook emphasized that they are still stressing the importance of SCAP 1.2 Validation.

An operating system vendor voiced concern regarding the way SCAP Validation is tied to specific versions of OVAL. Their new operating system contains features that are not currently supported by OVAL and is concerned that their customers would have to wait too long to be able to scan for it. Kim points to this exact issue as what she hopes to address at a developer days event this year. Kim also mentioned that if anyone has any other questions about the SCAP Validation Program, they should reach out to Melanie by sending a message to scap@nist.gov so that we can make sure to get more information out to the community. The same member also mentioned that while they don't think the whole picture is clear to them yet as long as there is an open dialog where they can ask questions, when they come up, they should be in good shape as the transition progresses. They also suggested that workshops would be a good way to do this.

Lastly, an OVAL Board member raised a concern about Software Identification tags (SWID tags)[5] and how they don't want to see them turn into a new scanning engine. Kim Watson explained how they need to get a better handle on what is policy and what does it need for asset collection, but, agrees entirely. Another member echoed this concern and did not want to have DHS reinvent the wheel. Kim Watson agreed.

Conclusion

The Board and Kim Watson both agreed that the proper messaging is vital to the success of this transition. Open lines of communication to provide feedback from both government and commercial

[5] http://tagvault.org/swid-tags/what-are-swid-tags/

representatives will be established to provide the best messaging and vision around this announcement. NIST has committed to hosting workshops and solidifying the importance of SCAP 1.2 Validation during these times. MITRE will continue to work with the OVAL Board to vote on bringing existing Sandbox features into OVAL 5.11 to reduce as many gaps in collection as possible.

As this discussion had occupied the entirety of the 2nd quarter OVAL Board Meeting with no discussion on the remainder of the agenda, a secondary phone call will be set up.

Action Items

1. OVAL Board to hold follow-up Board Call to complete remainder of agenda.