The Challenges of Writing OVAL Definitions

The challenges of developing good host-based assessment content and the opportunities afforded by using OVAL.

Writing good OVAL Definitions can be difficult due to the underlying need to research and describe a known good or bad system state. However, the research necessary to sufficiently understand a known good or bad system state is a challenge that is independent of OVAL. There is a required skill set needed to develop OVAL Definitions for a platform, and knowledge of the OVAL Language is only a small component. Furthermore, by providing a standard format for describing a known good or bad system state OVAL can help software vendors and researchers collaborate in investigating the detailed system information that is needed.

Required Skills for Writing an OVAL Definition

There is a specific skill set required to write good OVAL Definitions that often times does not align with the skill set needed to develop higher level configuration policy. In order to effectively write OVAL Definitions the author must be able to:

- Read and understand XML Documents
- Read and understand XML Schema
- Operate command line XML Schema validation tools and or posses an integrated development environment for XML
- Possibly understand and write XPath and regular expressions

There are emerging efforts to simplify the OVAL Definition development process. The basic approaches to this problem have been to develop editors to remove the need to understand XML, XML Schema, and XML Schema validation. The goal in developing an authoring capability is to allow content authors to focus on the difficult research problem and leverage their domain expertise to write good content without also needing to know both how to write XML as well as fully understand how the OVAL XML languages work. Additionally, the OVAL Team is working to provide guidance and other resources to further reduce the OVAL Language learning curve and simplify the process of developing good OVAL Definitions.

While it is important to understand the skill set needed to hand write OVAL Definitions, focusing solely on hand-developing content is a mistake. There are numerous use cases for OVAL in which automatically generating content based upon some data feed is the best approach. This has successfully been demonstrated by Red Hat for years (https://redhat.com/oval/). This same approach has been used in numerous other projects. If it is not possible to fully automate the generation of OVAL Definitions, it is often quite possible to generate most of it and then refine the content. This "generate and refine" approach was used to create all of the initial NIST FDCC SCAP benchmarks. These automated content generation approaches can dramatically reduce the actual OVAL Definition writing effort.

Researching System Configuration Information

Determining how to accurately check for an issue (patch or vulnerability presence, installed application, compliant configuration, etc) is a difficult research problem. There are a number of issues that make this process difficult:

- Software vendors are inconsistent across platforms and naturally change their practices over time. This makes the process of developing and testing low level system checks extremely difficult, particularly when a given definition is required to conduct the same tests across multiple versions of a vendor product.
- It is often the case that the software vendors have the detailed information needed to develop accurate checks for an issue, but either do not share this information at all or do not share the information in a format that lends itself to easy development of accurate checks.
- It is often the case that there is no single group within a software vendor that is the source of all the needed checking information around a product. In large software companies there tend to be groups with different responsibilities that may be aligned around products, vulnerability handling and response, secure configuration development, or other roles. Depending on the organizational structure these various groups may or may not have normal business reasons for communicating this detailed system state information.

Clearly, software vendors are key in this research process and their help is needed. An open standardized format for exchanging this information, like OVAL, allows these software vendors to share this information, but education and outreach is needed to demonstrate the value and importance of these vendors sharing this information.

Duplication of Efforts and Inconsistent Assessment Results

Some third-party software vendors develop enterprise security management products that may assess, report, and remediate systems in an enterprise. These and other enterprise management activities are dependent upon a thorough understanding of known good and bad system states. The software vendors in this field either leverage shared content for checking these known systems states or develop their own proprietary content. In developing their own content these vendors must employ teams of domain experts that know the internals of the systems they plan to write content for and manage substantial test environments to ensure accurate content is developed. There are numerous organizations that have these content development teams developing content in proprietary formats similar to OVAL. When these content teams develop their own content they frequently produce different and inconsistent solutions to the same problem. This inconsistency leads to inconsistent and inaccurate results across third party vendor products. Having a standardized format like OVAL, allows these cross vendor teams to share content and collaborate in the development of accurate checking content.

Organizations responsible for developing and publishing configuration policies (PCI DSS, USGCB, DISA STIG, etc.) typically provide high level guidance for how to securely configure systems, address vulnerabilities, or otherwise configure a system. This guidance is interpreted by each third party configuration management tool in use and then systems can be inspected to ensure conformance as appropriate. If this guidance is not published in an open standard format like OVAL, the work to research and describe low level system checks for conformance is simply pushed down stream to the third party vendors that help manage systems. This results in duplicated effort among organizations and inconsistent and inaccurate results across different third party tools.

Enabling Federated Enterprises

Enterprises rarely have single enterprise security management solutions. It is far more common that organizations have adopted a federated approach and deployed best of breed solutions for managing the systems of subordinate organizations. Additionally, it is commonly accepted that maintaining secure hardware and software configurations (see *20 Critical Security Controls for Effective Cyber Defense*, http://www.sans.org/critical-security-controls/) is key to the security of an enterprise. As such, organizations develop their own configuration policies that address organization specific needs. These policies may be organically developed or based upon other known good policies like those published by the Center for Internet Security. Here too these policies must be specified in such way that the third party vendors can assess systems for conformance with the policy. If the choice is made to express this organizational policy without detailed system configuration checks then the third party tools must carry the burden of translating the policy into the detailed system checks. This translation process will lead to inaccuracies and inconsistencies in addition to duplication of efforts across third party tool vendors. If an open standardized format like OVAL is used then one policy can be shared across the enterprise regardless of the third party management tool in use, as long as the tools understand the standard format.

Conclusion

Developing good host-based assessment content is a difficult research problem. Unfortunately people often incorrectly conflate the effort needed to write an OVAL Definition and the research needed to know what to write about. Developing OVAL Definitions is not trivial. However, writing the OVAL Definitions is only a small piece of the problem. The much greater challenge is determining how to check for a known good or bad system state. Vendors can help the community by providing detailed information in an open standardized format, like OVAL. Researchers that leverage OVAL can collaborate in the development of good host-based assessment content and share the research burden. Furthermore, having an open standardized format allows organizations to develop expertise and specialize in developing host-based assessment content. Investing in developing OVAL Definitions for host-based assessment can assist in tackling this challenge by reducing these duplicated research efforts, providing the opportunity for organizations to specialize in and offer content development services, and enable broad sharing of this information.