Security Automation Developer Days

March 22-25, 2011

Portrait Room
The National Institute for Standards and Technology
Gaithersburg, MD

Agenda

Tuesday, March 22nd, 2011

8:30 – 8:45 **Welcome** David Waltermire, NIST

8:45 – 10:20 **XCCDF Profiles** Charles Schmidt, MITRE

The community has requested, on multiple occasions, a review of the previous community decision not to support external profiles. The objective of this discussion will be to decide upon a structure to support external profiles or, if the community re-confirms its previous decision that no new structures are needed, develop a canonical procedure which would support equivalent functionality.

10:20 – 10:30 **Morning Break**

10:30 – 12:00 **Expanded Applicability Language** Jim Ronayne

Discuss evolving the CPE language into a more general applicability language that might include other schemas and let one better define a benchmark, profile, group, or rule. The goal would be to reduce the need for humans to manually figure out which benchmark to run against which hosts. This applicability language could also be used with other efforts including: remediation and vulnerability/configuration data feeds.

12:00 – 1:00 **Lunch** NIST Cafeteria

12:15 – 1:00 **Briefing: Asset Identification and ARF** Adam Halbardier, Booz Allen

Present information on the current state of the Asset Identification and Asset Reporting Format (ARF) efforts.

1:00 – 2:50 **Adv. Tailoring and Automated Profile Selection** Charles Schmidt, MITRE

Among the current open issues currently tracked against the XCCDF specification, some have sweeping implications related to the following: the expansion of XCCDF to include branches within its tailoring procedures, and structures that could support automated selection of profiles. This discussion will look at possible proposals for each of these with the objective of identifying specific changes to make to XCCDF to support the desired functionality.

2:50 – 3:00 **Afternoon Break**

3:00 – 4:45 **Other Open XCCDF Issues** Charles Schmidt, MITRE

This discussion will look at some of the recently raised issues and evaluate possible proposals for their resolution. The objective of this discussion will be to identify specific features that should be

Agenda (Continued)

included or rejected and, in the former case, the specific changes to the XCCDF specification and schema needed to support them.

4:45 – 5:00 **Wrap Up** David Waltermire, NIST

Wrap up the events of the day. Preview the next day. Make any announcements.

5:00 – 6:00 **Briefing: SCAP activities in Japan** Masato Terada, IPA

The speaker will provide an overview of the Japan Vulnerability Notes (JVN) website and its adoption of SCAP to provide vulnerability information related to software used within Japan. This session will cover the MyJVN security capabilities: Filtered Vulnerability Countermeasure Information Tool, Version Checker, the MyJVN Security Configuration Checker and the MyJVN APIs.

6:30 – 7:30 **BoF: Developing Security Automation Vocabularies** Paul Cichonski, NIST

This birds of a feather will continue the ongoing discussion relating to the use of W3C semantic technology within Security Automation. The focus will be on using RDF constructs to develop a draft security automation vocabulary that captures disparate security automation viewpoints spanning multiple domains. Due to the time constraints we will be having this BOF at a local restaurant; to ensure that enough space is reserved. Please contact Paul Cichonski (paul.cichonski@nist.gov) if you are interested in attending.

Wednesday, March 23rd, 2011

8:30 – 8:45 **Welcome** David Waltermire, NIST

8:45 – 10:15 **XCCDF Findings** Dick Whitehurst, McAfee

XCCDF Benchmarks currently provide useful information about the compliance of systems evaluated, but provide only is compliant or is not compliant results for each tested configuration item. In many cases, this is not enough information to be able to remediate the systems for those configuration items deemed not compliant. In some cases, it is useful to know why a system is considered either in compliance or not in compliance.

10:15 – 10:25 **Morning Break**

10:25 – 12:30 **Other Open XCCDF Issues** Charles Schmidt, MITRE

Continue discussion from the previous day.

12:30 – 1:30 **Lunch** NIST Cafeteria

1:30 – 2:00 **Demo: Automation Content Repository** David Waltermire

This discussion will start with a brief demo of a possible approach for managing and distributing SCAP content. After the demo will be a discussion on the approach and requirements for future capabilities.

2:00 – 3:20 **Automation Content Repositories** Kent Landfield, McAfee

Today we have created a standardized content format used by multiple SCAP tools from multiple vendors. What we have not addressed is the actual distribution of standardized content. Organizations are developing, customizing and tailoring content without a means to distribute, reuse and manage it. For larger sites with multiple SCAP products, changes to content can be painful in

Agenda (Continued)

assuring all the SCAP products are using and reporting on the same content. This discussion will focus on defining requirements for creating a standardized means for accessing and distributing content from a central service within an organization.

3:20 – 3:30 **Afternoon Break**

3:30 – 4:45 **Automation Content Repositories** Kent Landfield, McAfee

Continue previous discussion.

4:45 – 5:00 **Wrap Up** David Waltermire, NIST

Wrap up the events of the day. Preview the next day. Make any announcements.

5:30 – 8:00 **S O C I A L**

Thursday, March 24th, 2011

8:30 – 8:45 **Welcome** David Waltermire, NIST

8:45 – 10:30 **Content Development Best Practices** Kent Landfield, McAfee

There are many areas of content development that are problematic. Content developers vary in the quality of content they produce mainly due to not having a means for lessons learned to be propagated. This session will focus discussion on identifying best practices and how best to capture them.

10:30 – 10:45 **Morning Break**

10:45 – 12:00 **OCIL in the Enterprise** Gerry McGuire, MITRE

Discuss enhancements to OCIL to address enterprise use cases. During this session representatives from industry and government will lead the discussion around possible approaches.

12:00 – 12:30 **Integration of Asset Identification in OVAL** Matt Hansbury, MITRE

Discuss using the new specification in OVAL.

12:30 – 1:30 **Lunch** NIST Cafeteria

12:45 – 1:30 **Briefing: An Operational Implementation of CPE** Joe Wolfkiel, DISA

This discussion provides an overview of how the DoD is implementing CPE in the discovery, reporting, and management of installed software and update inventories. The speaker will discuss existing implementations of CPE, as well as implementation guidance provided to the US Army for implementation on their Configuration Management Database, and on the US Government developed Asset Configuration Compliance Module (ACCM).

1:30 – 2:30 **Implement the Notion of One Test** Jasen Jacobsen, MITRE

This would include defining a test in the oval-definitions-schem.xsd and then deprecating all others tests. This would include deprecating the <ind-def:unknown_test/>. We could replace this test with an unknown criterion in the oval-def:definition/oval-def:criteria section. This sort of change would reduce the overall burden of developing schema for new system constructs, reduce our schema bloat, reduce essentially duplicate schema constructs, and possibly make some implementations simpler.

Agenda (Continued)

2:30 – 3:15 **OVAL & TPM Demo and Discussion** Charles Schmidt, MITRE

Review a brief demonstration of an extension of the OVAL Langue to utilize the TPM and then consider adding a proposed TPM component schema to support the demonstrated capabilities.

3:15 – 3:25 **Afternoon Break**

3:25 – 4:00 **variable_instance Attribute - Deprecate or Fix?** Jon Baker, MITRE

Discuss the variable_instance attribute as it is defined in the oval-system-characteristics-schema and oval-results-schemas and its shortcomings. Then consider the implications of either fixing the mask attribute or simply deprecating it and working to remove it from the language.

4:00 – 4:30 **MAEC & OVAL** Ivan Kirillov, MITRE

This talk will introduce the connection between MAEC and OVAL in order to help the OVAL community better understand why there are open feature requests for mutex and file signature checking and prepare the community for other similar feature requests to support the MAEC observables use case. A brief overview of the relevant aspects of MAEC will be followed by a discussion of MAEC observables and current need for new OVAL Tests.

4:30 – 4:45 **Wrap Up** David Waltermire, NIST

Wrap up the events of the day. Preview the next day. Make any announcements.

4:45 – 5:30 **Demo: DoD Remediation Reference Implementation** SEI and SPAWAR

- *Step through a demonstration of DoD reference implementation using straw-man example data.*
- *Examine implementation details of sample Remediation Manager.*
- *Discuss considerations when building future reference implementations.*
- *Discussion period: Request for suggestions and comments from the community*

5:30 – 6:30 **BoF: Using TNC and SCAP Together** Steve Hanna, Juniper Networks

The Trusted Network Connect (TNC) standards seem to mesh well with SCAP. The TNC standards provide protocols for querying devices as to compliance status. SCAP provides standard data formats and enumerations valuable for such queries. We'll bring TNC and SCAP experts together for an interactive discussion of how these standards should best be integrated.

Friday, March 25th, 2011

8:30 – 8:45 **Welcome** David Waltermire, NIST

8:45 – 12:30 **Remediations Standardization Discussion** Gerry McGuire, MITRE

- *Goals and objectives of Remediation Standards development.*
- *Major discussion in reference to:*
  - *Common Remediation Enumeration (CRE) and Extended Remediation Information (ERI) standards*
  - *Remediation Policy*
  - *Remediation Tasking*
- *Challenges and questions for the community*
- *Request for suggestions and comments from the community*

Agenda (Continued)

12:30 – 1:30 **Lunch** NIST Cafeteria

1:30 – 2:00 **New Functions - unique, count, and others?** Matt Hansbury, MITRE

Discuss proposals for a count and unique function in the oval-definitions-schema and consider other possible additions for version 5.10.

2:00 – 2:30 **mask Attribute - Deprecate or Fix?** Danny Haynes, MITRE

Discuss the mask attribute as it is defined in the oval-definitions-schema and its shortcomings. Then consider the implications of either fixing the mask attribute or simply deprecating it and working to remove it from the language.

2:30 – 3:00 **Error Handling in Variables** Danny Haynes, MITRE

A review of the current error handling process when computing a variable value is currently defined and a discussion of the shortcomings. Once the current issues are understood the conversation will focus on reviewing a proposal to address the problem and the implications of the proposal.

3:00 – 3:15 **Wrap Up** David Waltermire, NIST

Wrap up the events of the day and the week. Make any announcements.