Security Automation and Continuous Monitoring
Internet-Draft
Intended status: Informational
Expires: September 8, 2016

M. Cokus
D. Haynes
D. Rothenberg
The MITRE Corporation
J. Gonzalez
Department of Homeland Security

March 7, 2016

OVAL(R) Variables Model
draft-haynes-sacm-oval-variables-model-00

Abstract

This document specifies Version 5.11.1 of the OVAL Variables Model which contains constructs that allow for the specification of values for external_variables defined in content that was created using the OVAL Definitions Model. The OVAL Variables Model serves as a useful mechanism for parameterizing content based on the OVAL Definitions Model.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 8, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The Open Vulnerability and Assessment Language (OVAL) [OVAL-WEBSITE] is an international, information security community effort to standardize how to assess and report upon the machine state of systems. For over ten years, OVAL has been developed in collaboration with any and all interested parties to promote open and publicly available security content and to standardize the representation of this information across the entire spectrum of security tools and services.

OVAL provides an established framework for making assertions about an system's state by standardizing the three main steps of the assessment process: representing the current machine state; analyzing the system for the presence of the specified machine state; and representing the results of the assessment which facilitates collaboration and information sharing among the information security community and interoperability among tools.

This draft is part of the OVAL contribution to the IETF SACM WG that standardizes the representation used to analyze a system for the presence of a specific machine state. It is intended to serve as a starting point for the endpoint posture assessment data modeling needs of SACM specifically for creating parameterized Collection and Evaluation Guidance.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. oval_variables

The oval_variables type defines the base structure in the OVAL Variables Model for representing a collection of OVAL Variables and their associated values. This container type adds metadata about the origin of the content and allows for a signature.

Property	Type	Count	Description
generator	oval:GeneratorType	1	Information regarding the generation of the OVAL Variables content. The timestamp property of the generator MUST represent the time at which the oval_variables was created.
variables	VariablesType	1	The variables defined in the OVAL Variables content.
signature	ext:Signature	0..1	Mechanism to ensure the integrity and authenticity of the OVAL Variables content.

Table 1: oval_variables Construct

3. VariablesType

The VariablesType provides a container for one or more OVAL Variables.

Property	Type	Count	Description
variable	VariableType	1..*	A collection of OVAL Variables.

Table 2: VariablesType Construct

4. VariableType

The VariableType defines a variable in the OVAL Variables Model that corresponds to an instance of an external variable in content based on the OVAL Definitions Model.

Property	Type	Count	Description
id	oval:VariableIDPattern	1	The globally unique identifier of an external variable.
datatype	oval:SimpleDatatypeEnumeration	1	The datatype of the value(s) in the variable.
comment	string	1	The documentation associated with the variable instance.
value	string	1..*	The value(s) associated with the variable.

Table 3: VariableType Construct

5. OVAL Variables Model Schema

The XML Schema that implements this OVAL Variables Model can be found below.

```
          <?xml version="1.0" encoding="utf-8"?>
   <xsd:schema
     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
     xmlns:oval-var="http://oval.mitre.org/XMLSchema/
     oval-variables-5"
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
     xmlns:sch="http://purl.oclc.org/dsdl/schematron"
     targetNamespace="http://oval.mitre.org/XMLSchema/
     oval-variables-5"
     elementFormDefault="qualified" version="5.11">
     <xsd:import
       namespace="http://oval.mitre.org/XMLSchema/oval-common-5"
       schemaLocation="oval-common-schema.xsd"/>
     <xsd:import
       namespace="http://www.w3.org/2000/09/xmldsig#"
       schemaLocation="xmldsig-core-schema.xsd"/>
     <xsd:annotation>
       <xsd:documentation/>
       <xsd:documentation>The following is a
         description of the elements, types, and
         attributes that compose the core schema for
         encoding Open Vulnerability and Assessment
         Language (OVAL) Variables. This schema is
         provided to give structure to any external
         variables and their values that an OVAL
         Definition is expecting.</xsd:documentation>
       <xsd:appinfo>
         <schema>Core Variable</schema>
         <version>5.11.1</version>
         <date>4/22/2015 09:00:00 AM</date>
         <terms_of_use>Copyright (C) 2010 United States Government.
           All Rights Reserved.</terms_of_use>
         <sch:ns prefix="oval-var"
           uri="http://oval.mitre.org/XMLSchema/oval-variables-5"
         />
       </xsd:appinfo>
     </xsd:annotation>
   <!-- ================================================== -->
   <!-- ================================================== -->
   <!-- ================================================== -->
     <xsd:element name="oval_variables">
       <xsd:annotation>
         <xsd:documentation>The oval_variables
           element is the root of an OVAL Variable
           Document. Its purpose is to bind together
           the different variables contained in the
           document. The generator section must be
```

```
          present and provides information about
          when the variable file was compiled and
          under what version. The optional Signature
          element allows an XML Signature as defined
          by the W3C to be attached to the document.
          This allows authentication and data
          integrity to be provided to the user.
          Enveloped signatures are supported. More
          information about the official W3C
          Recommendation regarding XML digital
          signatures can be found at
          http://www.w3.org/TR/xmldsig-core/.</xsd:documentation>
      </xsd:annotation>
      <xsd:complexType>
        <xsd:sequence>
          <xsd:element name="generator"
            type="oval:GeneratorType"/>
          <xsd:element name="variables"
            type="oval-var:VariablesType"
            minOccurs="0" maxOccurs="1"/>
          <xsd:element ref="ds:Signature"
            minOccurs="0" maxOccurs="1"/>
        </xsd:sequence>
      </xsd:complexType>
      <xsd:key name="varKey">
        <xsd:annotation>
          <xsd:documentation>Enforce uniqueness
            amongst the variable ids found in the
            variable document.</xsd:documentation>
        </xsd:annotation>
        <xsd:selector xpath=".//oval-var:variable"/>
        <xsd:field xpath="@id"/>
      </xsd:key>
    </xsd:element>
  <!-- ======================================================== -->
  <!-- ==================  GENERATOR  ========================== -->
  <!-- ======================================================== -->
    <!--
                 The GeneratorType is defined by the oval common
                 schema.  Please refer to that documentation for a
                 description of the complex type.
          -->
  <!-- ======================================================== -->
  <!-- =================  DEFINITIONS  ======================== -->
  <!-- ======================================================== -->
    <xsd:complexType name="VariablesType">
      <xsd:annotation>
        <xsd:documentation>The VariablesType complex
```

```
          type is a container for one or more
          variable elements. Each variable element
          holds the value of an external variable
          used in an OVAL Definition. Please refer
          to the description of the VariableType for
          more information about an individual
          variable.</xsd:documentation>
      </xsd:annotation>
      <xsd:sequence>
        <xsd:element name="variable"
          type="oval-var:VariableType" minOccurs="1"
          maxOccurs="unbounded"/>
      </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="VariableType">
      <xsd:annotation>
        <xsd:documentation>Each variable element
          contains the associated datatype and value
          which will be substituted into the OVAL
          Definition that is referencing this
          specific variable.</xsd:documentation>
        <xsd:documentation>The notes section of a
          variable should be used to hold
          information that might be helpful to
          someone examining the technical aspects of
          the variable. Please refer to the
          description of the NotesType complex type
          for more information about the notes
          element.</xsd:documentation>
      </xsd:annotation>
      <xsd:sequence>
        <xsd:element name="value"
          type="xsd:anySimpleType" minOccurs="1"
          maxOccurs="unbounded"/>
        <xsd:element name="notes"
          type="oval:NotesType" minOccurs="0"
          maxOccurs="1"/>
      </xsd:sequence>
      <xsd:attribute name="id"
        type="oval:VariableIDPattern" use="required"/>
      <xsd:attribute name="datatype" use="required"
        type="oval:SimpleDatatypeEnumeration">
        <xsd:annotation>
          <xsd:documentation>Note that the 'record'
            datatype is not permitted on
            variables.</xsd:documentation>
        </xsd:annotation>
      </xsd:attribute>
```

```
      <xsd:attribute name="comment"
        type="xsd:string" use="required"/>
    </xsd:complexType>
  <!-- ======================================================== -->
  <!-- ==================  SIGNATURE  ========================== -->
  <!-- ======================================================== -->
    <!--
                  The signature element is defined by the xmldsig
                  schema.  Please refer to that documentation for
                  a description of the valid elements and types.
                  More information about the official W3C
                  Recommendation regarding XML digital
                  signatures can be found at
                  http://www.w3.org/TR/xmldsig-core/.
          -->
  <!-- ======================================================== -->
  <!-- ======================================================== -->
  <!-- ======================================================== -->
  </xsd:schema>
```

6. Intellectual Property Considerations

Copyright (C) 2010 United States Government. All Rights Reserved.

DHS, on behalf of the United States, owns the registered OVAL trademarks, identifying the OVAL STANDARDS SUITE and any component part, as that suite has been provided to the IETF Trust. A "(R)" will be used in conjunction with the first use of any OVAL trademark in any document or publication in recognition of DHS's trademark ownership.

7. Acknowledgements

The authors wish to thank DHS for sponsoring the OVAL effort over the years which has made this work possible. The authors also wish to thank the original authors of this document Jonathan Baker, Matthew Hansbury, and Daniel Haynes of the MITRE Corporation as well as the OVAL Community for its assistance in contributing and reviewing the original document. The authors would also like to acknowledge Dave Waltermire of NIST for his contribution to the development of the original document.

8. IANA Considerations

This memo includes no request to IANA.

9. Security Considerations

While OVAL is just a set of data models and does not directly introduce security concerns, it does provide a mechanism by which to represent endpoint posture assessment information. This information could be extremely valuable to an attacker allowing them to learn about very sensitive information including, but, not limited to: security policies, systems on the network, criticality of systems, software and hardware inventory, patch levels, user accounts and much more. To address this concern, all endpoint posture assessment information should be protected while in transit and at rest. Furthermore, it should only be shared with parties that are authorized to receive it.

Another possible security concern is due to the fact that content expressed as OVAL has the ability to impact how a security tool operates. For example, content may instruct a tool to collect certain information off a system or may be used to drive follow-up actions like remediation. As a result, it is important for security tools to ensure that they are obtaining OVAL content from a trusted source, that it has not been modified in transit, and that proper validation is performed in order to ensure it does not contain malicious data.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

10.2. Informative References

[OVAL-WEBSITE] The MITRE Corporation, "The Open Vulnerability and Assessment Language", 2015, <http://ovalproject.github.io/>.

Authors' Addresses

Michael Cokus
The MITRE Corporation
903 Enterprise Parkway, Suite 200
Hampton, VA 23666
USA

Email: msc@mitre.org

Daniel Haynes
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: dhaynes@mitre.org

David Rothenberg
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: drothenberg@mitre.org

Juan Gonzalez
Department of Homeland Security
245 Murray Lane
Washington, DC 20548
USA

Email: juan.gonzalez@dhs.gov