Mask Attribute - Deprecate or Fix?

Danny Haynes

The MITRE Corporation

Overview

- Background
- How the mask attribute works
- Known issues
  - Masking values that you are not checking
  - Conflicting mask attribute values
  - Misplaced Schematron rule
  - Modifies the OVAL Definitions document
  - Overlap with the OVAL Results Directives
  - Other issues
- Wrap-up

Background

- Introduced in OVAL 5.3
- Goal of the mask attribute
  - Prevent sensitive information, that is needed for evaluation, from being disclosed to unauthorized parties
- Example
  - Check the minimum password length policy used by a system
    - May not want to pass this information along
- How is the mask attribute being used today?
  - Does anyone use the mask attribute in their content?
  - Do vendors support the mask attribute in their tools?
  - Challenges?

How the mask attribute works

- "*If the mask attribute is set to 'true', then the value of this field, along with the operation used, should not appear in the results file.*"
  [oval-def:EntityAttributeGroup/@mask]
  - The mask attribute can be specified on all object and state entities
  - The value and operation should be removed from all instances in the OVAL Results document (object, state, and item entities)

- "*A system characteristics file that is not held within a results file should not use the mask attribute.*" [oval-def:EntityAttributeGroup/@mask]
  - The OVAL System Characteristics document would become unusable

How the mask attribute works (continued)

- **OVAL Definitions Document**

```
<passwordpolicy_test id="oval:sample:tst:1" check="all" comment="Test the password policy.">
  <object object_ref="oval:sample:obj:1"/>
  <state state_ref="oval:sample:ste:1"/>
</passwordpolicy_test>

<passwordpolicy_object id="oval:sample:obj:1" comment="Collect the password policy settings."/>

<passwordpolicy_state id="oval:sample:ste:1"
                      comment="Minimum password length is greater than 14.">
  <min_passwd_len datatype="int" operation="greater than" mask="true">14</min_passwd_len>
</passwordpolicy_state>
```

How the mask attribute works (continued)

- **OVAL System Characteristics Document**

```
<passwordpolicy_item id="1">
  <max_passwd_age datatype="int">15552000</max_passwd_age>
  <min_passwd_age datatype="int">86400</min_passwd_age>
  <min_passwd_len datatype="int">3</min_passwd_len>
  <password_hist_len datatype="int">12</password_hist_len>
  <password_complexity datatype="boolean">1</password_complexity>
  <reversible_encryption datatype="boolean">0</reversible_encryption>
</passwordpolicy_item>
```

How the mask attribute works (continued)

- **OVAL Results Document**

```
<passwordpolicy_test check="all" comment="Test the password policy."  id="oval:sample:tst:1">
  <object object_ref="oval:sample:obj:1"/>
  <state state_ref="oval:sample:ste:1"/>
</passwordpolicy_test>

<passwordpolicy_object comment="Collect the password policy settings." id="oval:sample:obj:1"/>


<passwordpolicy_state comment="Minimum password length is greater than 14."
id="oval:sample:ste:1">
  <min_passwd_len datatype="int"/>
</passwordpolicy_state>


<passwordpolicy_item id="1">
  <max_passwd_age datatype="int">15552000</max_passwd_age>
  <min_passwd_age datatype="int">86400</min_passwd_age>
  <min_passwd_len datatype="int"/>
  <password_hist_len datatype="int">12</password_hist_len>
  <password_complexity datatype="boolean">1</password_complexity>
  <reversible_encryption datatype="boolean">0</reversible_encryption>
</passwordpolicy_item>
```

Masking values that you are not checking

- Want to check to see when a user's password was last changed
  - unix-def:shadow_test can check this information
    - Encrypted passwords are also collected!

```
<shadow_state id="oval:sample:ste:1" comment="...">
  <password mask="true" operation="pattern match"/>
  <chg_lst datatype="int" operation="greater than">14000</chg_lst>
</shadow_state>
```

- Must write the entity so that it does not affect evaluation
  - `<chg_lst datatype="int" operation="greater than or equal">0</chg_lst>`
  - `<file_read_attributes datatype="boolean" var_check="only one" var_ref="oval:sample:var:1" />`
  - Very awkward

Conflicting mask attribute values

```
<file_test id="oval:sample:tst:1" check="all">
  <object object_ref="oval:sample:obj:1"/>
  <state state_ref="oval:sample:ste:1"/>
</file_test>
```

```
<file_object id="oval:sample:obj:1">
  <path>/tmp</path>
  <filename mask="true">sample.txt</filename>
</file_object>
```

```
<file_state id="oval:sample:ste:1">
  <filename mask="false">sample.txt</filename>
</file_state>
```

- **No documentation regarding what to do here**
  - **Take the safe approach and always mask**

Misplaced Schematron rule

```
<sch:rule context="oval-sc:system_data/*/*|
                   oval-sc:system_data/*/*/*">
  <sch:assert test="not(@mask) or @mask='false' or .=''">
    item <sch:value-of select="../@id":/> - a value for the
    <sch:value-of select="name()"/> entity should only be
    supplied if the mask attribute is 'false'
  </sch:assert>
</sch:rule>
```

Reminder: "A system characteristics file that is not held within a results file should not use the mask attribute."

- **Used to enforce the masking of all item entities**
- **We do not want to enforce this in a standalone OVAL System Characteristics document**
  - **We need to enforce this in an OVAL Results document**
- **Let's move it to the OVAL Results schema**

```
<sch:rule
  context="/oval-res:oval_results/oval-res:results/oval-res:system/oval-sc:system_data/*/*|
           /oval-res:oval_results/oval-res:results/oval-res:system/oval-sc:system_data/*/*/*">
  <sch:assert test="not(@mask) or @mask='false' or .=''">item <sch:value-of select="../@id"/>
  - a value for the <sch:value-of select="name()"/> entity should only be supplied if the mask
  attribute is 'false'</sch:assert>
</sch:rule>
```

Modifies the OVAL Definitions document

Reminder: "The value and operation should be removed from all instances in the OVAL Results document (object, state, and item entities)."

- **Original OVAL Definitions document**

```
<textfilecontent54_object id="oval:sample:obj:1">
  <filepath>/etc/sensitive-config.txt</filepath>
  <pattern mask="true" operation="pattern match">password=(*)</pattern>
  <instance mask="true" datatype="int">1</instance>
</textfilecontent54_object>
```

- **OVAL Definitions document in the OVAL Results document**

```
<textfilecontent54_object id="oval:sample:obj:1">
  <filepath>/etc/sensitive-config.txt</filepath>
  <pattern mask="true"/>
  <instance mask="true" datatype="int"/>
</textfilecontent54_object>
```

- **Validation Errors**
  - ***The datatype for the instance entity is 'int' but the value is not an integer***
  - ***Operation attribute for the pattern entity of a textfilecontent54_object should be 'pattern match'***
- **Changes the meaning of the OVAL Definition**
  - **Does not accurately describe what was checked**
  - **Invalidates signature**

Overlap with the OVAL Results Directives

- OVAL Results Directives were introduced in OVAL 5.0
  - Allows users to specify what level of detail is reported in the OVAL Result document
  - Expanded in OVAL 5.8
- include_source_definitions = "false" (default directives)
  - Remove the entire source OVAL Definitions document from the OVAL Results document
- content = "thin" (default and class directives)
  - Include the ID and evaluation result of the OVAL Definition
  - Exclude the criteria and system characteristics information associated with the OVAL Definition
- Is the level of granularity provided by the mask attribute needed?
  - Are OVAL Results Directives sufficient?
  - Are there other solutions that can help us here?

Other issues

- **Comments may hurt you**
  - `<passwordpolicy_state id="..." comment="Minimum password length is greater than 14.">`
- **XCCDF uses OVAL**
  - **Tailoring values may or may not appear in XCCDF Results**
    - **Community is generally including the tailoring values**

Wrap-up

- Is this a valuable feature for the community?
  - Do we need to make improvements?
  - Should we deprecate it?
  - Do we need a different solution?
- Any other questions, comments, or concerns?