-------------------------------------------------------------------------------------

OVAL Proposal Form

-------------------------------------------------------------------------------------

The OVAL Proposal Form is used by members of the community to prepare proposals for migration into an official release of OVAL. The form will be critical in helping the members of the community understand, review, and vet proposals.

Once an OVAL Proposal Form is submitted to the oval-developer-list, the OVAL Moderator will review and verify the proposal for completeness at which point it will be ready for community review and discussion.

When a new proposal is introduced to the community, the OVAL Moderator will work with the OVAL Board to determine the impact of the proposal. If the proposal is deemed a high impact change, it must be developed in the OVAL Sandbox which will require the completion of this form as well as an OVAL Board vote before it is migrated into an official release. More information about the OVAL Board Voting Process can be found at [1]. If the proposal is deemed a low impact change, the proposed change can be made directly to an official OVAL release.

Please direct any questions or concerns to MITRE at [oval@mitre.org](mailto:oval@mitre.org).

-------------------------------------------------------------------------------------

Steps to Take

-------------------------------------------------------------------------------------

1) Review the OVAL Language Sandbox page [2] and the Requesting Changes to the OVAL Language page [3].

2) Complete the form provided below.

3) Email the completed form to the oval-developer-list at [oval-developer-list@lists.mitre.org](mailto:oval-developer-list@lists.mitre.org) with a subject of "FOR REVIEW: <Proposal Name> Proposal Form".

4) Revise the proposal, as needed, based on community discussion and feedback.

-------------------------------------------------------------------------------------

Contact Information

-------------------------------------------------------------------------------------

1) Name: Michael Peck

2) Email Address: mpeck@mitre.org

3) Phone Number (optional):

-------------------------------------------------------------------------------------

Introduction to Proposal

-------------------------------------------------------------------------------------

1) What is the new capability?

The OVAL schemas for Android provide a standards-based capability to check Android device configuration.

2) Why is the new capability needed?

The Android OVAL schemas are needed to provide a standards-based capability to check Android device configuration.

3) What is the version of the targeted official OVAL release?

The targeted OVAL version for this proposal is OVAL 5.11.

-------------------------------------------------------------------------------------

Benefits of Proposal

-------------------------------------------------------------------------------------

1) How does the proposal relate to existing OVAL use cases [4]?

The tests provide capabilities to express and assess Android device configuration for the following OVAL use cases:

* Configuration Management
* Vulnerability Assessment

2) What does this proposal enable that cannot currently be accomplished in the OVAL Language?

The OVAL Language does not currently include any Android-specific schemas. The OVAL SQL tests could potentially be used to query device state information held by a mobile device management system, but such an approach is not desired because it assumes a particular mechanism for gathering Android device state information, would require creating customized SQL tests for each particular mobile device management product, and the storage mechanisms of each mobile device management product are often proprietary. Instead we prefer an approach that abstracts the details of how Android device state information is obtained and stored.

The proposed Android schema provides the ability to check (not an exhaustive list):

* Installed applications
  + Application name, version, permissions, X.509 certificate belonging to the application developer
* Bluetooth settings
* Camera policy settings
* Installed trusted certificates (trust anchors)
* Screen lock policies
  + Screen lock timeout
  + Lockscreen widget policy
* Various device settings
  + USB debugging enabled/disabled
  + Mock location enabled/disabled
  + Allow installation of applications from unknown sources enabled/disabled
  + List of applications that hold privileged device administrator access
  + Automatic date/time network synchronization enabled/disabled
  + Automatic time zone network synchronization enabled/disabled
  + USB mass storage enabled/disabled
* Device encryption settings
* Location service information
* Network configuration information
* Password policy settings
* Device characteristics
  + Model, manufacturer, OS version, whether a hardware-backed keystore is present, and related information
* Wi-Fi configuration information
* Telephony information

3) What alternative approaches for supporting these use cases were considered and why is this one the best?

OVAL SQL tests are an alternative approach, but for the reasons stated above we do not believe that is the optimal approach.

Numerous mobile device management products exist today that provide the ability to assess Android device configuration. However, there is currently no standards-based mechanism to input to these products the compliance checks to perform or to output compliance results.

-------------------------------------------------------------------------------------

Impacts of Proposal

-------------------------------------------------------------------------------------

1) Which existing OVAL schemas are affected by this proposal?

None.

2) Does the proposal break backward compatibility with previous versions? Please see OVAL Versioning Policy [5] for more information.

This proposal does not break backward compatibility.

2) How will the proposed changes impact OVAL content authors?

This will provide OVAL content authors with the ability to create new content based on the new tests. We have created proof-of-concept OVAL definitions demonstrating the ability to automate useful compliance checks.

For example:

<https://github.com/OVALProject/Sandbox/blob/master/resources/x-android-schema/content/android-stig_v2.xml>

<https://github.com/OVALProject/Sandbox/blob/master/resources/x-android-schema/content/android-stig_v2.html>

<https://github.com/OVALProject/Sandbox/blob/master/resources/x-android-schema/content/test-knox-stig.xml>

<https://github.com/OVALProject/Sandbox/blob/master/resources/x-android-schema/content/test-knox-stig.html>

Example system characteristics:

<https://github.com/OVALProject/Sandbox/blob/master/resources/x-android-schema/content/android-system-char-20140422-galaxynexus.xml>

3) How will the proposed changes impact OVAL content consumers?

No impact to current OVAL content consumers. These changes will provide an opportunity to use OVAL to create Android configuration management and vulnerability assessment content.

4) How will the proposed changes impact existing OVAL content?

No impact.

5) How will the proposed changes impact existing OVAL implementations?

The impact will depend on whether the existing OVAL implementations need to implement Android-specific schema features. In many cases it will not be necessary.

If mobile device management products choose to implement OVAL support, they will need to add the capability to parse Android OVAL definitions and assess gathered mobile device state information against the definitions. Mobile device management systems typically already include the ability to gather device state information, but they will need to ensure they are collecting the particular information used by the Android OVAL schema.

We created a proof-of-concept Android application that gathers device state information and outputs Android OVAL system characteristics. For proof-of-concept testing, the Android OVAL system characteristics and Android OVAL definitions can be inputted into the ovaldi OVAL interpreter for assessment on another system without requiring any modifications to ovaldi itself.

6) Are there any concerns regarding this proposal (e.g., undocumented APIs, etc.)? If so, are there any mitigating factors?

No. As demonstrated by our proof-of-concept Android application, there is no dependence on undocumented APIs. Some APIs are only available on newer versions of Android. Our application demonstrates the ability to check what version of Android it is running on and only call the APIs that are available.

-------------------------------------------------------------------------------------

Technical Review

-------------------------------------------------------------------------------------

1) Do the schema changes follow the accepted naming and design conventions?

Yes.

2) Do the schema changes satisfy the requirements specified in the Requesting Changes to the OVAL Language page [3]?

Yes.

3) Do the schema changes align with the targeted official release (e.g., changes that break backward compatibility should not target a minor release)? Please see the OVAL Versioning Policy [5] for more information.

Yes.

4) Have the new capabilities been successfully implemented and tested with sample content?

Yes.

-------------------------------------------------------------------------------------

Resource Information

-------------------------------------------------------------------------------------

1) Provide URLs for relevant OVAL Sandbox Issues:

N/A

2) Provide URLs for OVAL Sandbox schemas that exemplify the proposed changes:

<https://github.com/OVALProject/Sandbox/blob/master/x-android-definitions.xsd>

<https://github.com/OVALProject/Sandbox/blob/master/x-android-system-characteristics.xsd>

3) Provide URLs for the location of sample OVAL Definitions, OVAL System Characteristics, and OVAL Results that exemplify the proposed changes:

Sample OVAL Definitions:

<https://github.com/OVALProject/Sandbox/blob/master/resources/x-android-schema/content/android-stig_v2.xml>

<https://github.com/OVALProject/Sandbox/blob/master/resources/x-android-schema/content/android-test.xml>

<https://github.com/OVALProject/Sandbox/blob/master/resources/x-android-schema/content/test-knox-stig.xml>

4) Provide URLs for products or tools that implement the proposed changes:

Example Android application (source and binary) for gathering OVAL System Characteristics:

<https://github.com/OVALProject/Sandbox/tree/master/resources/x-android-schema/code>

5) Provide URLs to any other resources that may be relevant to reviewing and verifying the proposal:

N/A

-------------------------------------------------------------------------------------

References

-------------------------------------------------------------------------------------

[1] <http://oval.mitre.org/community/board/voting.html>

[2] <http://oval.mitre.org/language/sandbox.html>

[3] <http://oval.mitre.org/language/about/change_requests.html>

[4] <http://oval.mitre.org/adoption/usecasesguide.html>

[5] <http://oval.mitre.org/language/about/versioning.html>