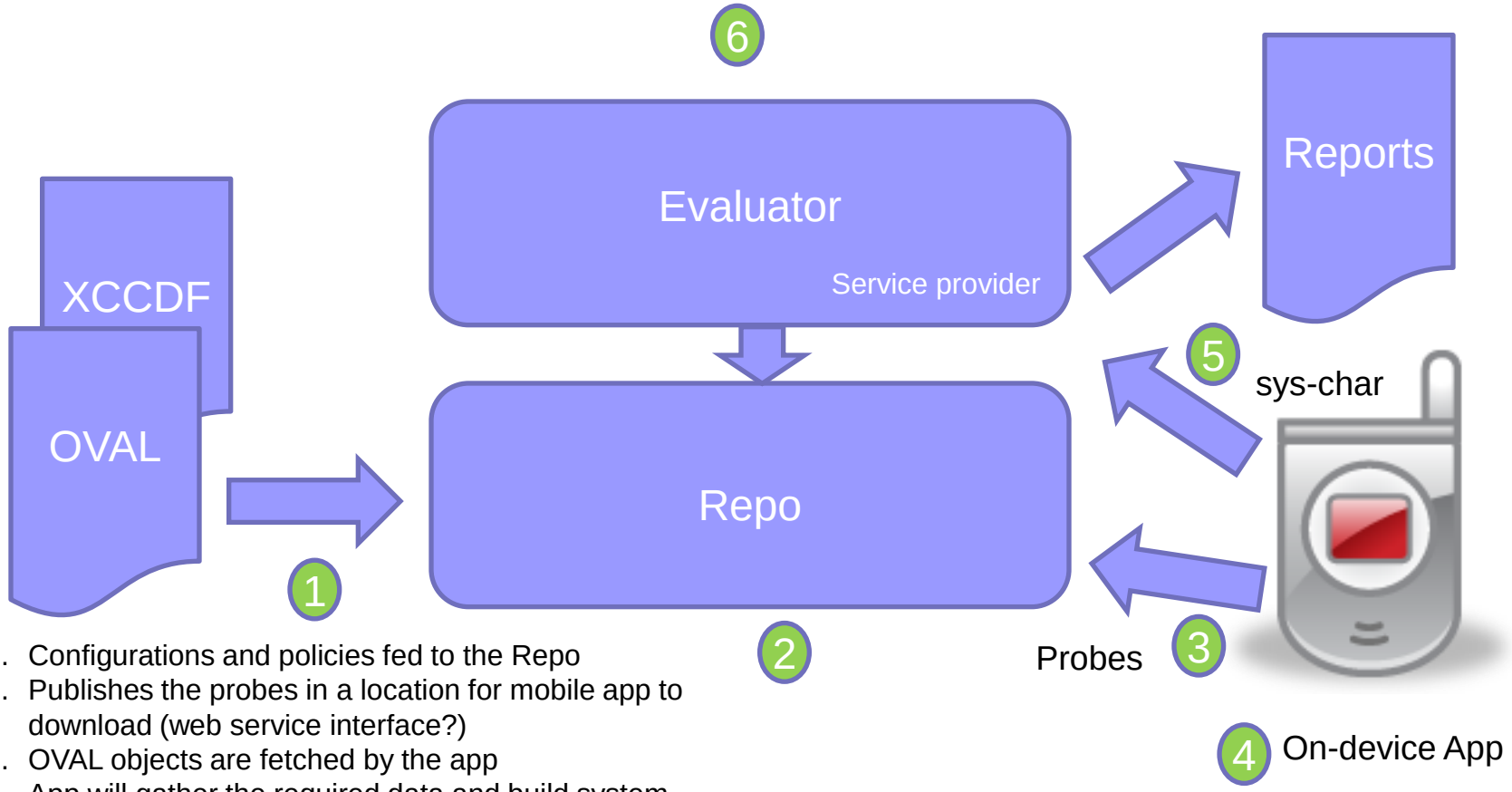
OVAL Android Schema

Chandrashekhar Basavanna

bchandra@secpod.com

Demo



1. Configurations and policies fed to the Repo
2. Publishes the probes in a location for mobile app to download (web service interface?)
3. OVAL objects are fetched by the app
4. App will gather the required data and build system-characteristics
5. App will push the system-characteristics to the evaluator
6. Evaluator performs assessment and generates the reports. Report status can be fetched by the device or view the report over the URL.

Goal

- OVAL covers majority of the Operating Systems
- Network devices coverage is getting extended
- Next step is to bring Mobile devices into SCAP space
- Build POC, develop OVAL test content
- Acceptance into the official OVAL release
- Develop content and extend the coverage in SecPod SCAP Repo

Different Approaches

- Different Android versions, multiple vendor tweaked versions
- MDM vs. An App based implementation
- The approach taken to design the schema:
  - Keep the implementation details outside the scope
  - Keep in mind “vanilla” Android
  - Drive the need for “probes” based on the current benchmark guides, published CVEs

List of probes

- system_details_test
- camera_test
- password_test
- encryption_test
- device_access_test
- location_service_test
- wifi_test
- wifi_security_test
- bluetooth_test
- app_manager_test
- network_test

More Probes

- unix-def:file_test
- ind-def:filehash58_test
- linux-def:partition_test
- ind-def:textfilecontent54_test
- linux-def:environmentvariable_test

Challenges

- Unable to implement due to technical reasons

browser_security_test

flashboot_version_test

adb_system_test

Challenges

- Hurdles because of OVAL's incapability? **None**
- OVAL family need to be defined, using "undefined" currently

Test Content

- Search results from SCAP Repo:
  - “android cve” – Matches: 186
  - "google android" cpe – Matches: 20
- OVAL Android Schema – in the Sandbox
- OVAL Definitions – covers 10 CVEs and 10 Compliance based
- CCE and XCCDF – to be done
- Content will be available for download at www.scaprepo.com

Credit

Thanks to:

MITRE team

Tim Nary, Tim Harrison: B.A.H