OVAL Reporting

Charles Schmidt

May 4, 2010

History

- In FY 07, MITRE developed the Report Schema for NSA
- In FY 09, MITRE used internal funding to revise and present the Open Checklist Reporting Language (OCRL)
  - Write-ups distributed on NIST's emerging-specs mail list
  - Presentation at the June Security Automation Developer Days
    - Feedback was to reuse existing standards by binding to OVAL
- In FY09 & FY10, MITRE converted OCRL to the OVAL Reports language
  - MITRE internal and DHS funding
  - New schema in OVAL (like Definitions and System Characteristics)
- First full draft of the language published April 14, 2010

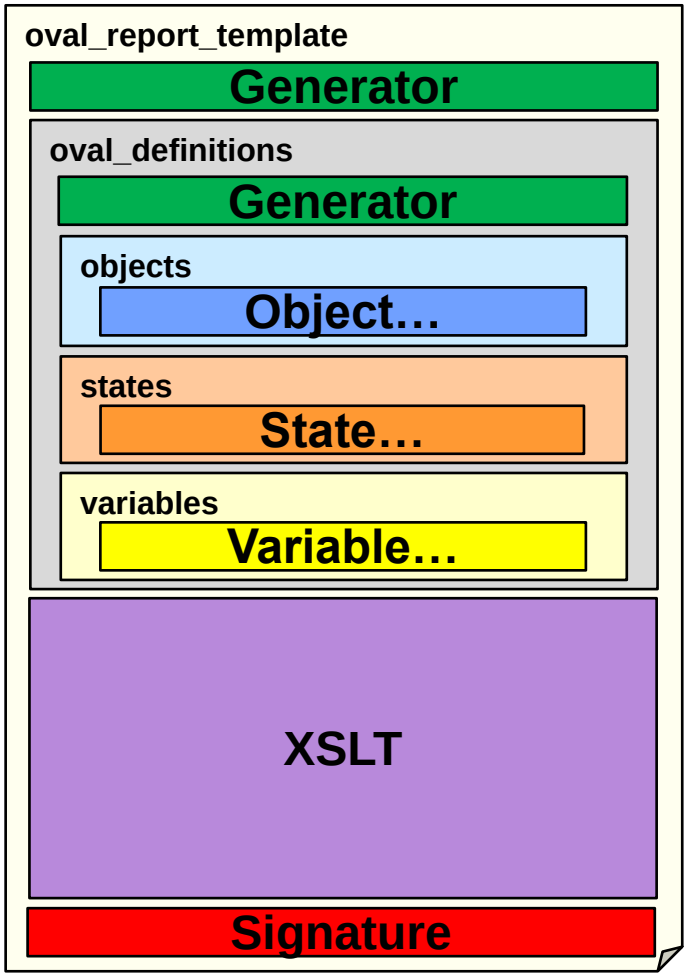
What does OVAL Reporting do?

1. Collect information about a system
   - E.g., registry key values, file permissions, etc.
2. Format that information into a report
   - Supports correlation of data from multiple sources
   - Can output in any text-based format (text, HTML, XML, etc.)

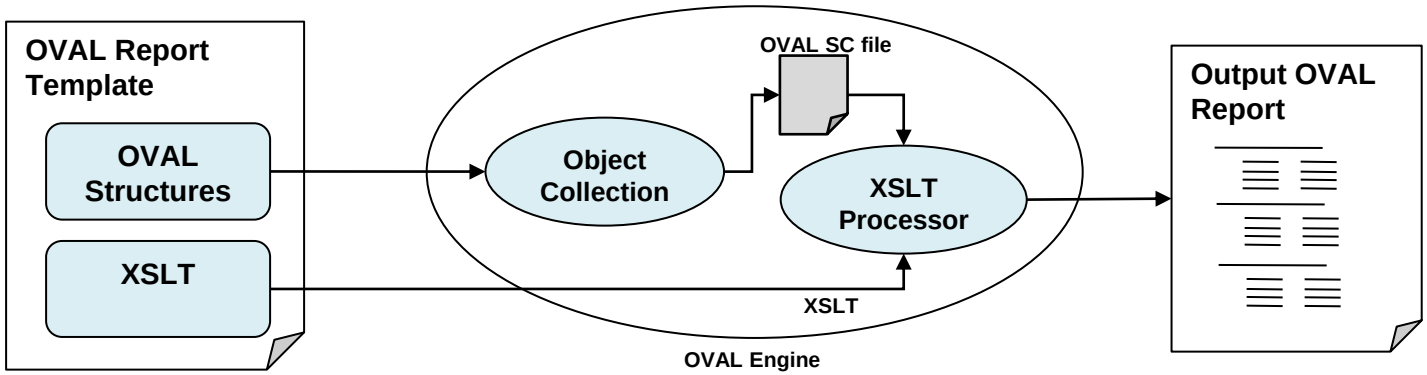
- Individual report templates (source files) can be named as references
  - Allows XCCDF to use checks to generate reports
- Report templates will be processed by OVAL Definition Interpreters

OVAL Report Template Structure

- **Generator**
  - Metadata about file construction
- **OVAL Block**
  - OVAL Objects, States, and Variables
  - Guides data collection
- **XSLT Block**
  - XSLT 1.0 content
  - Guides data organization and formatting
- **Signature**
  - Optional digital signature



OVAL Report Template Processing



- Start with an OVAL Report Template
  - Contains OVAL Structures and XSLT
- OVAL structures are sent to the OVAL Engine
  - Objects are collected
  - An OVAL System Characteristics (SC) file is produced
- SC file and XSLT portion of the Report Template are passed to a basic XSLT processor
- The XSLT processor produces the output report

Challenges

- Soliciting community input
  - Some input received after request-for-comments
- Addressing broadening of use cases
  - Interest in similar capabilities for OCIL
  - Interest in final result roll-up/summary result generation
- Fitting to OVAL conventions
  - OVAL's extensive body of material imposes design conventions that have been challenging to meet at times

Deliveries

- Request for comments – January 5, 2010
  - High-level design overview
- OVAL Reports Schema – April 14, 2010
  - Prototype OVAL Schema
- Creating an OVAL Report Template – April 14, 2010
  - Documentation on using the OVAL Reports Schema
  - Includes an example report template
- OVAL Reports Template Library – April 14, 2010
  - A library of helper XSLT templates that can be invoked by authors to perform common tasks

Moving Forward

- Solicit community feedback
  - Language is of interest to MITRE benchmark development teams
  - Would like other input
  - Modify language to address community concerns
- Update of the OVALDI reference implementation to process OVAL Reports
- Possible inclusion in OVAL as soon as OVAL 5.8 (August 2010)

Questions?